# CRIMINAL JUSTICE INFORMATION AND PROTECTION OF PRIVACY ACT OF 1975

## HEARINGS

BEFORE THE

## SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS

OF THE

## COMMITTEE ON THE JUDICIARY
## UNITED STATES SENATE

NINETY-FOURTH CONGRESS

FIRST SESSION

ON

**S. 2008, S. 1427, and S. 1428**

JULY 15 AND 16, 1975

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
56-833 O WASHINGTON : 1975

# CRIMINAL JUSTICE INFORMATION AND PROTECTION OF PRIVACY ACT OF 1975

## HEARINGS

BEFORE THE

## SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS

OF THE

## COMMITTEE ON THE JUDICIARY
## UNITED STATES SENATE

NINETY-FOURTH CONGRESS

FIRST SESSION

ON

**S. 2008, S. 1427, and S. 1428**

JULY 15 AND 16, 1975

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
56-833 O WASHINGTON : 1975

COMMITTEE ON THE JUDICIARY

JAMES O. EASTLAND, Mississippi, *Chairman*

JOHN L. McCLELLAN, Arkansas
PHILIP A. HART, Michigan
EDWARD M. KENNEDY, Massachusetts
BIRCH BAYH, Indiana
QUENTIN N. BURDICK, North Dakota
ROBERT C. BYRD, West Virginia
JOHN V. TUNNEY, California
JAMES ABOUREZK, South Dakota

ROMAN L. HRUSKA, Nebraska
HIRAM L. FONG, Hawaii
HUGH SCOTT, Pennsylvania
STROM THURMOND, South Carolina
CHARLES McC. MATHIAS, JR., Maryland
WILLIAM L. SCOTT, Virginia

---

SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS

JOHN V. TUNNEY, California, *Chairman*

JOHN L. McCLELLAN, Arkansas
EDWARD M. KENNEDY, Massachusetts
BIRCH BAYH, Indiana
PHILIP A. HART, Michigan
JAMES ABOUREZK, South Dakota

HUGH SCOTT, Pennsylvania
ROMAN L. HRUSKA, Nebraska
HIRAM L. FONG, Hawaii
STROM THURMOND, South Carolina

JANE L. FRANK, *Chief Counsel*
DOUGLASS LEA, *Counsel*
LYDIA GRIEG, *Chief Clerk*
JOSEPH P. ALLEN, *Clerk*

# CONTENTS

## HEARING DAYS



## STATEMENTS BY SUBCOMMITTEE MEMBERS



## WITNESSES



## PREPARED STATEMENTS



## BILLS SUBMITTED FOR THE RECORD



## MISCELLANEOUS

## APPENDIX

### Additional Statements



### Articles for the Record



### Correspondence

# CRIMINAL JUSTICE INFORMATION AND PROTECTION OF PRIVACY ACT OF 1975

TUESDAY, JULY 15, 1975

U.S. Senate,
Subcommittee on Constitutional Rights,
of the Committee on the Judiciary,
*Washington, D.C.*

The subcommittee met, pursuant to notice, at 9:35 a.m., in room 2228, Dirksen Senate Office Building, Senator John V. Tunney (chairman of the subcommittee) presiding.

Present: Senators Tunney, Kennedy, Hruska, and Thurmond.

Also present: Jane L. Frank, chief counsel; Douglass Lea, majority counsel; J. C. Argetsinger, minority counsel.

Senator Tunney. The subcommittee will come to order.

## OPENING STATEMENT OF HON. JOHN V. TUNNEY, A U.S. SENATOR FROM THE STATE OF CALIFORNIA; CHAIRMAN, SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS

Senator Tunney. With these hearings we enter the final stages of this subcommittee's exhaustive consideration of the legislative proposals to regulate the flow of criminal justice information and to protect the privacy and other constitutional rights of individuals upon whom such information is collected.

The bill now under consideration, S. 2008, represents 4 years of extensive investigation by the Subcommittee on Constitutional Rights. It is the culmination of our concerted efforts to develop a reasonable and balanced solution to the concerns articulated over the years by both civil libertarians and local law enforcement officials.

More specifically, the bill now before you represents a compromise between two earlier bills, S. 1427 and S. 1428, which I introduced in April. Those two earlier bills expressed the most advanced thinking on this complicated subject by Senator Ervin and the Justice Department.

In developing S. 2008, I think we have gone a long way toward combining and harmonizing the best features of the Ervin and Justice bills. It is still not a perfect bill, and I hope the hearings today and tomorrow will help us to give it a final polish.

Four years ago we began our journey with a rather simple discovery, uncontrolled dissemination of incomplete, and often inaccurate, police rap sheets have an enormous potential to stigmatize the lives of citizens—many of them totally innocent of any crimes—who come into contact with the criminal justice system.

We soon learned, however, that we were entering a very complicated world, one that was rapidly becoming computerized and one that was inherently linked with such issues as privacy, Federal-State relations, due process, the concentration of police powers and freedom of the press.

It was only during the last Congress, when Senators Ervin and Hruska introduced comprehensive criminal justice information legislation, that we began to address the full range of these issues.

Undoubtedly the chief catalyst in our thinking was the realization of the extent to which crime information had already been computerized and was, therefore, widely available and on an instantaneous basis.

We also began to realize that computerization had been accompanied by an almost total focus on efficiency. Concern for the future of individual rights had received little attention. In addition, new issues—such as the highly technical problem of who shall control criminal justice system message switching—continue to emerge.

We still have no overall framework for dealing with these new and complex issues.

The legislation now before us provides such a framework. It establishes minimum Federal standards for the use and dissemination of criminal justice information and allows the States, through their own legislative processes and their control of the Oversight Commission created by this bill, to determine their own priorities in this area of public policymaking.

I would like to emphasize the last point: This legislation returns power to the States.

Thus it is appropriate that our first witness is a State official with responsibilities in this area.

At this time I would like to submit S. 2008, with its section-by-section analysis, and S. 1427 and S. 1428, for the record.

[The above referred to bills follow:]

94TH CONGRESS
1ST SESSION

# S. 2008

IN THE SENATE OF THE UNITED STATES

JUNE 24 (legislative day, JUNE 6), 1975

Mr. TUNNEY introduced the following bill; which was read twice and referred to the Committee on the Judiciary

# A BILL

To protect the constitutional rights and privacy of individuals upon whom criminal justice information has been collected and to control the collection and dissemination of criminal justice information, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,* That this Act may be cited as the "Criminal Justice Information Control and Protection of Privacy Act of 1975".

## TITLE I—PURPOSE AND SCOPE

### FINDINGS

SEC. 101. The Congress hereby finds and declares that—

(a) The responsible maintenance, use, and dissemination of complete and accurate criminal justice information



★(Star Print)

among criminal justice agencies is recognized as necessary and indispensable to effective law enforcement and criminal justice and is encouraged.

(b) The irresponsible use or dissemination of inaccurate or incomplete information, however, may infringe on individual rights.

(c) While the enforcement of criminal laws and the regulation of criminal justice information is primarily the responsibility of State and local government, the Federal Government has a substantial and interconnected role.

(d) This Act is based on the powers of the Congress—

(1) to place reasonable restrictions on Federal activities and upon State and local governments which receive Federal grants or other Federal services or benefits, and

(2) to facilitate and regulate interstate commerce.

DEFINITIONS

SEC. 102. As used in this Act—

(1) "Automated" means utilizing electronic computers or other automatic data processing equipment, as distinguished from performing operations manually.

(2) "Dissemination" means any transfer of information, whether orally, in writing, or by electronic means.

(3) "The administration of criminal justice" means any activity by a criminal justice agency directly involving the

apprehension, detention, pretrial release, posttrial release, prosecution, defense, adjudication, or rehabilitation of accused persons or criminal offenders or the collection, storage, dissemination, or usage of criminal justice information.

(4) "Criminal justice agency" means a court or any other governmental agency or subunit thereof which as its principal function performs the administration of criminal justice and any other agency or subunit thereof which performs criminal justice activities but only to the extent that it does so.

(5) "Criminal justice information" means arrest record information, nonconviction record information, conviction record information, criminal history record information, and correctional and release information. The term does not include criminal justice investigative information or criminal justice intelligence information.

(6) "Arrest record information" means notations of arrest, detention, indictment, filing of information, or other formal criminal charge on an individual which does not include the disposition arising out of that arrest, detention, indictment, information, or charge.

(7) "Criminal history record information" means arrest record information and any disposition arising therefrom.

(8) "Conviction record information" means criminal history record information disclosing that a person has

disclosing that

inal charges or

luded, abandoned,

formation" means in-

connection with bail

proceedings, reports on the

of an alleged offender, reports

participants in rehabilitation programs,

reports.

criminal justice investigative information" means

with an identifiable individual com-

agency in the course of conduct-

of a specific criminal act including

criminal act derived from re-

interviews, or from any type of

not include criminal justice in-

formation nor does it include initial reports filed by a criminal justice agency describing a specific incident, not indexed or accessible by name and expressly required by State or Federal statute to be made public.

(13) "Criminal justice intelligence information" means information associated with an identifiable individual compiled by a criminal justice agency in the course of conducting an investigation of an individual relating to possible future criminal activity of an individual, or relating to the reliability of such information, including information derived from reports of informants, investigators, or from any type of surveillance. The term does not include criminal justice information nor does it include initial reports filed by a criminal justice agency describing a specific incident, not indexed or accessible by name and expressly required by State or Federal statute to be made public.

(14) "Judge of competent jurisdiction" means (a) a judge of a United States district court or a United States court of appeals; (b) a Justice of the Supreme Court of the United States; (c) a judge of any court of general criminal jurisdiction in a State; or (d) for purposes of section 208 (b) (5), any other official in a State who is authorized by a statute of that State to enter orders authorizing access to sealed criminal justice information.

(15) "Attorney General" means the Attorney General of the United States.

(16) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

APPLICABILITY

SEC. 103. (a) This Act applies to criminal justice information, criminal justice investigative information, or criminal justice intelligence information maintained by criminal justice agencies—

(1) of the Federal Government,

(2) of a State or local government and funded in whole or in part by the Federal Government,

(3) which exchange information interstate, and

(4) which exchange information with an agency covered by paragraph (1), (2), or (3) but only to the extent of that exchange.

(b) This Act applies to criminal justice information, criminal justice intelligence information and criminal justice investigative information obtained from a foreign government or an international agency to the extent such information is commingled with information obtained from domestic sources. Steps shall be taken to assure that, to the maximum extent feasible, whenever any information subject to this Act is provided to a foreign government or an international

agency, such information is used in a manner consistent with the provisions of this Act.

(c) The provisions of this Act do not apply to—

(1) original books of entry or police blotters, whether automated or manual, maintained by a criminal justice agency at the place of original arrest or place of detention, not indexed or accessible by name and required to be made public;

(2) court records of public criminal proceedings or official records of pardons or paroles or any index thereto organized and accessible by date or by docket or file number, or organized and accessible by name so long as such index contains no other information than a cross reference to the original pardon or parole records by docket or file number;

(3) Public criminal proceedings and court opinions, including published compilations thereof;

(4) records of traffic offenses maintained by departments of transportation, motor vehicles, or the equivalent, for the purpose of regulating the issuance, suspension, revocation, or renewal of drivers' licenses;

(5) records relating to violations of the Uniform Code of Military Justice but only so long as those records are maintained solely within the Department of Defense; or

(6) statistical or analytical records or reports in which individuals are not identified and from which their identities are not ascertainable.

## TITLE II—COLLECTION AND DISSEMINATION OF CRIMINAL JUSTICE INFORMATION, CRIMINAL JUSTICE INVESTIGATIVE INFORMATION, AND CRIMINAL JUSTICE INTELLIGENCE INFORMATION

### DISSEMINATION, ACCESS, AND USE OF CRIMINAL JUSTICE INFORMATION—CRIMINAL JUSTICE AGENCIES

SEC. 201. (a) With limited exceptions hereafter described, access to criminal justice information, criminal justice investigative information, and criminal justice intelligence information shall be limited to authorized officers or employees of criminal justice agencies, and the use or further dissemination of such information shall be limited to purposes of the administration of criminal justice.

(b) The use and dissemination of criminal justice information shall be in accordance with criminal justice agency procedures reasonably designed to insure—

(1) that the use or dissemination of arrest record information or nonconviction record information is restricted to the following purposes—

(A) The screening of an employment application or review of employment by a criminal justice

agency with respect to

cants;

(B) The collation

mination of pretrial

the adjudication of

preparation of a pre

(C) The supe

agency of an indi

to the custody

arrest

(D) The investigation of an individual when that individual has already been arrested or detained.

(E) The development of investigative leads concerning an individual who has not been arrested, when there are specific and articulable facts which, taken together with rational inferences from those facts, warrant the conclusion that the individual has committed or is about to commit a criminal act and the information requested may be relevant to that act,

(F) The alerting of an official or employee of a criminal justice agency that a particular individual may present a danger to his safety, or

(G) Similar essential purposes to which the in-

formation is relevant as defined in the procedures prescribed pursuant to the section; and

(2) that correctional and release information is disseminated only to criminal justice agencies; or to the individual to whom the information pertains, or his attorney, where authorized by Federal or State statute, court rule, or court order.

IDENTIFICATION AND WANTED PERSON INFORMATION

SEC. 202. Personal identification information, including fingerprints, voice prints, photographs, and other physical descriptive data, may be used or disseminated for any official purpose, but personal identification information which includes arrest record information or criminal history record information may be disseminated only as permitted by this Act. Information that a person is wanted for a criminal offense and that judicial process has been issued against him, together with an appropriate description and other information which may be of assistance in locating the person or demonstrating a potential for violence, may be disseminated for any authorized purpose related to the administration of criminal justice. Nothing in this Act prohibits direct access by a criminal justice agency to automated wanted person information.

DISSEMINATION, ACCESS AND USE OF CRIMINAL JUSTICE INFORMATION—NONCRIMINAL JUSTICE AGENCIES

SEC. 203. (a) Except as otherwise provided by this Act, conviction record information may be made available for purposes other than the administration of criminal justice only if expressly authorized by Federal or State statute.

(b) Arrest record information indicating that an indictment, information, or formal charge was made against an individual within twelve months of the date of the request for the information, and is still pending, may be made available for a purpose other than the administration of criminal justice if expressly authorized by Federal or State statute. Arrest record information made available pursuant to this subsection may be used only for the purpose for which it was made available and may not be copied or retained by the requesting agency beyond the time necessary to accomplish that purpose.

(c) When conviction record information or arrest record information is requested pursuant to subsections (a) or (b), the requesting agency or individual shall notify the individual to whom the information relates that such information about him will be requested and that he has the

56-833 O - 75 - 2

right to seek review of the information prior to its dissemination.

(d) Criminal justice information may be made available to qualified persons for research related to the administration of criminal justice.

(e) A criminal justice agency may disseminate criminal justice information, upon request, to officers and employees of the Immigration and Naturalization Service, consular officers, and officers and employees of the Visa Office of the Department of State, who require such information for the purpose of administering the immigration and nationality laws. The Attorney General and the Secretary of State shall adopt internal operating procedures reasonably designed to insure that arrest record information received pursuant to this subsection is used solely for the purpose of developing further investigative leads and that no decision adverse to an individual is based on arrest record information unless there has been a review of the decision at a supervisory level.

(f) A criminal justice agency may disseminate criminal justice information, upon request, to officers and employees of the Bureau of Alcohol, Tobacco, and Firearms, the United States Customs Service, the Internal Revenue Service and the Office of Foreign Assets Control of the Department of the Treasury, who require such information for the purpose

of administering those laws under their respective jurisdictions. The Attorney General and the Secretary of the Treasury shall adopt internal operating procedures reasonably designed to insure that arrest record information received pursuant to this subsection is used solely for the purpose of developing further investigative leads and that no decision adverse to an individual is based on arrest record information unless there has been a review of the decision at a supervisory level.

(g) The Drug Enforcement Administration of the United States Department of Justice may disseminate criminal record information to federally registered manufacturers and distributors of controlled substances for use in connection with the enforcement of the Controlled Substances Administration Act.

(h) Nothing in this Act prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, if such disclosure is reasonably contemporaneous with the event to which the information relates. Nor is a criminal justice agency prohibited from confirming prior arrest record information or criminal record information to members of the news media or any other person, upon specific inquiry as

to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by section 103 (b) from the application of this Act.

DISSEMINATION, ACCESS, AND USE OF CRIMINAL JUSTICE INFORMATION—APPOINTMENTS AND EMPLOYMENT INVESTIGATIONS

SEC. 204. (a) A criminal justice agency may disseminate criminal justice information, whether or not sealed pursuant to section 208, criminal justice intelligence information, and criminal justice investigative information to a Federal, State, or local government official who is authorized by law to appoint or nominate judges, executive officers of law enforcement agencies or members of the Commission on Criminal Justice Information created under section 301 or any State board or agency created or designated pursuant to section 307, and to any legislative body authorized to approve such appointments or nominations. The criminal justice agency shall disseminate such information concerning an individual only upon notification from the appointing or nominating official that he is considering that individual for such an office, or from the legislative body that the individual has been nominated for the office, and that the individual has

been notified of the request for such information and has given his written consent to the release of the information.

(b) A criminal justice agency may disseminate arrest record information and criminal history record information to an agency of the Federal Government for the purpose of an employment application investigation, an employment retention investigation, or the approval of a security clearance for access to classified information, when the Federal agency requests such information as a part of a comprehensive investigation of the history and background of an individual, pursuant to an obligation to conduct such an investigation imposed by a Federal statute or Federal executive order, and pursuant to agency regulations setting forth the nature and scope of such an investigation. Arrest record information or criminal history record information that has been sealed may be made available only for the purpose of the approval of a security clearance. For investigations concerning security clearances for access to information classified as top secret, criminal justice intelligence information and criminal justice investigative information may be made available pursuant to this subsection. At the time he files his application, seeks a change of employment status, applies for a security clearance, or otherwise causes the initiation of the investigation, the individual shall be put on notice

that such an investigation will be conducted and that access to this type of information will be sought.

(c) Any information made available pursuant to this section may be used only for the purpose for which it is made available and may not be redisseminated, copied, or retained by the requester beyond the time necessary to accomplish the purpose for which it was made available.

SECONDARY DISSEMINATION OF CRIMINAL JUSTICE INFORMATION

SEC. 205. Any agency or individual having access to, or receiving criminal justice information is prohibited, directly or through any intermediary, from disseminating such information to any individual or agency not authorized to have such information; except that correctional officials of criminal justice agencies, with the consent of an individual under their supervision to whom the information refers, may orally represent the substance of the individual's criminal history record information to prospective employers or other individuals if they believe that such representation may be helpful in obtaining employment or rehabilitation for the individual.

METHOD OF ACCESS TO CRIMINAL JUSTICE INFORMATION

SEC. 206. (a) Except as provided in section 203 (d) or in subsection (b) of this section, a criminal justice agency may disseminate arrest record information or criminal his-

tory record information only if the inquiry is based upon identification of the individual to whom the information relates by means of name and other personal identification information. After the arrest of an individual, such information concerning him shall be available only on the basis of positive identification of him by means of fingerprints or other equally reliable identification record information.

(b) Notwithstanding the provisions of subsection (a), a criminal justice agency may disseminate arrest record information and criminal history record information for criminal justice purposes where inquiries are based upon categories of offense or data elements other than personal identification information if the criminal justice agency has adopted procedures reasonably designed to insure that such information is used only for the purpose of developing investigative leads for a particular criminal offense and that the individuals to whom such information is disseminated have a need to know and a right to know such information.

SECURITY, ACCURACY, AND UPDATING OF CRIMINAL JUSTICE INFORMATION

SEC. 207. (a) Each criminal justice agency shall adopt procedures reasonably designed at a minimum—

(1) to insure the physical security of criminal justice information, to prevent the unauthorized disclosure of the information, and to insure that the criminal justice in-

formation is currently and accurately revised to include subsequently received information and that all agencies to which such information is disseminated or from which it is collected are currently and accurately informed of any correction, deletion, or revision of the information;

(2) to insure that criminal justice agency personnel responsible for making or recording decisions relating to dispositions shall as soon as feasible report such dispositions to an appropriate agency or individual for inclusion with arrest record information to which such dispositions relate;

(3) to insure that records are maintained and kept current for at least three years with regard to—

(A) requests from any other agency or person for criminal justice information, the identity and authority of the requester, the nature of the information provided, the nature, purpose, and disposition of the request, and pertinent dates; and

(B) the source of arrest record information and criminal history information; and

(4) to insure that criminal justice information may not be submitted, modified, updated, or removed from any criminal justice agency record or file without verification of the identity of the individual to whom the information refers and an indication of the person or

agency submitting, modifying, updating, or removing the information.

(b) If the Commission on Criminal Justice Information finds that full implementation of this section is infeasible because of cost or other factors it may exempt the provisions of this section from application to information maintained prior to the effective date of this Act.

SEALING AND PURGING OF CRIMINAL JUSTICE INFORMATION

SEC. 208. (a) Each criminal justice agency shall adopt procedures providing at a minimum—

(1) for the prompt sealing or purging of criminal justice information when required by State or Federal statute, regulation, or court order;

(2) for the prompt sealing or purging of criminal justice information relating to an offense by an individual who has been free from the jurisdiction or supervision of any criminal justice agency for a period of seven years, if the individual has previously been convicted and such offense is not specifically exempted from sealing by a Federal or State statute;

(3) for the sealing or purging of arrest record information after a period of two years following an arrest, detention, or formal charge, whichever comes first, if no conviction of the individual occurred during that period,

no prosecution is pending at the end of the period, and the individual is not a fugitive; and

(4) for the prompt purging of criminal history record information in any case in which a law enforcement agency has elected not to refer a case to the prosecutor [illegible] information, seeking the issuance of criminal charge.

(b) Criminal justice information [illegible] section may be made available—

(1) in connection with research pursuant to subsection 203(d);

(2) in connection with a review by the individual or his attorney pursuant to section 209;

(3) in connection with an audit conducted pursuant to section 304 or 310;

(4) where a conviction record has been sealed and an indictment, information, or other formal criminal charge is subsequently filed against the individual; or

(5) where a criminal justice agency has obtained an access warrant from a State judge of competent jurisdiction if the information sought is in the possession of a State or local agency, or from a Federal judge of competent jurisdiction if the information sought is in the possession of a Federal agency. Such warrants may

be issued as a matter of discretion by the judge in cases in which probable cause has been shown that (A) such access is imperative for purposes of the criminal justice agency's responsibilities in the administration of criminal justice, and (B) the information sought is not reasonably available from any other source or through any other method.

(c) Access to any index of sealed criminal justice information shall be permitted only to the extent necessary to implement subsection (b). Any index of sealed criminal justice information shall consist only of personal identification information and the location of the sealed information.

ACCESS BY INDIVIDUALS TO CRIMINAL JUSTICE INFORMATION FOR PURPOSES OF CHALLENGE

SEC. 209. (a) Any individual shall, upon satisfactory verification of his identity and compliance with applicable rules or regulations, be entitled to review any arrest record information or criminal history record information concerning him maintained by any criminal justice agency and to obtain a copy of it if needed for the purpose of challenging its accuracy or completeness or the legality of its maintenance.

(b) Each criminal justice agency shall adopt and publish rules or regulations to implement this section.

(c) The final action of a criminal justice agency on a

request to review and challenge criminal justice information in its possession as provided by this section, or a failure to act expeditiously on such a request, shall be reviewable pursuant to a civil action under section 308.

(d) No individual who, in accord with this section, obtains information regarding himself may be required or requested to show or transfer records of that information to any other person or any other public or private agency or organization.

CRIMINAL JUSTICE INTELLIGENCE INFORMATION

SEC. 210. (a) Criminal justice intelligence information may be maintained by a criminal justice agency only for official criminal justice purposes. It shall be maintained in a physically secure environment and shall be kept separate from criminal justice information.

(b) Criminal justice intelligence information regarding an individual may be maintained only if grounds exist connecting such individual with known or suspected criminal activity and if the information is pertinent to such criminal activity. Criminal justice intelligence information shall be reviewed at regular intervals, but at a minimum whenever dissemination of such information is requested, to determine whether such grounds continue to exist, and if grounds do not exist such information shall be purged.

(c) Within the criminal justice agency maintaining the

information, access to criminal justice intelligence information shall be limited to those officers or employees who have both a need to know and a right to know such information.

(d) Criminal justice intelligence information may be disseminated from the criminal justice agency which collected such information only to a Federal agency authorized to receive the information pursuant to section 204 or to a criminal justice agency which needs the information to confirm the reliability of information already in its possession or for investigative purposes if the agency is able to point to specific and articulable facts which taken together with rational inferences from those facts warrant the conclusion that the individual has committed or is about to commit a criminal act and that the information may be relevant to the act.

(e) When access to criminal justice intelligence information is permitted under subsection (c) or when such information is disseminated pursuant to subsection (d) a record shall be kept of the identity of the person having access or the agency to which information was disseminated, the date of access or dissemination, and the purpose for which access was sought or information disseminated. Such records shall be retained for at least three years.

(f) Direct remote terminal access to criminal justice intelligence information shall not be permitted. Remote terminal access shall be permitted to personal identification infor-

mation sufficient to provide an index of subjects of criminal justice intelligence information and the names and locations of criminal justice agencies possessing criminal justice intelligence information concerning such subjects and automatically referring the requesting agency to the agency maintaining more complete information.

(g) An assessment of criminal justice intelligence information may be provided to any individual when necessary to avoid imminent danger to life or property.

CRIMINAL JUSTICE INVESTIGATIVE INFORMATION

SEC. 211. (a) Criminal justice investigative information may be maintained by a criminal justice agency only for official law enforcement purposes. It shall be maintained in a physically secure environment and shall be kept separate from criminal justice information. It shall not be maintained beyond the expiration of the statute of limitations for the offense concerning which it was collected or the sealing or purging of the criminal justice information related to such offense, whichever occurs later.

(b) Criminal justice investigative information may be disclosed pursuant to subsection 552(b)(7) of title 5 of the United States Code or any similar State statute, or pursuant to any Federal or State statute, court rule, or court order permitting access to such information in the course of court proceedings to which such information relates.

(c) Except when such information is available pursuant to subsection (b), direct access to it shall be limited to those officers or employees of the criminal justice agency which maintains the information who have a need to know and a right to know such information and it shall be disseminated only to other governmental officers or employees who have a need to know and a right to know such information in connection with their civil or criminal law enforcement responsibilities. Records shall be kept of the identity of persons having access to criminal justice investigative information or to whom such information is disseminated, the date of access or dissemination, and the purpose for which access is sought or files disseminated. Such records shall be retained for at least three years.

(d) Criminal justice investigative information may be made available to officers and employees of government agencies for the purposes set forth in section 204.

## TITLE III—ADMINISTRATIVE PROVISIONS; REGULATIONS, CIVIL REMEDIES; CRIMINAL PENALTIES

### COMMISSION ON CRIMINAL JUSTICE INFORMATION

SEC. 301. CREATION AND MEMBERSHIP.—(a) There is hereby created a Commission on Criminal Justice Information (hereinafter the "Commission") which shall have overall responsibility for the administration and enforcement

of this Act. The Commission shall be composed of thirteen members. One of the members shall be the Attorney General and two of the members shall be designated by the President as representatives of other Federal agencies outside of the Department of Justice. One of the members shall be designated by the President on the recommendation of the Judicial Conference of the United States. The nine remaining members shall be appointed by the President with the advice and consent of the Senate. Of the nine members appointed by the President, seven shall be officials of criminal justice agencies from seven different States at the time of their nomination, representing to the extent possible all segments of the criminal justice system. The two remaining Presidential appointees shall be private citizens well versed in the law of privacy, constitutional law, and information systems technology, and shall not have been employed by any criminal justice agency within the five years preceding their appointments. Not more than seven members of the Commission shall be of the same political party.

(b) The President shall designate one of the seven criminal justice agency officials as Chairman and such designation shall also be confirmed by the advice and consent of the Senate. The Commission shall elect a Vice Chairman who shall act as Chairman in the absence or disability of the Chairman or in the event of a vacancy in that office.

(c) The designated members of the Commission shall serve at the will of the President. The Attorney General and the appointed members shall serve for terms of five years. Any vacancy shall not affect the powers of the Commission and shall be filled in the same manner in which the original appointment or designation was made.

(d) Seven members of the Commission shall constitute a quorum for the transaction of business.

SEC. 302. COMPENSATION OF MEMBERS.—(a) Each member of the Commission who is not otherwise in the service of the Government of the United States shall receive a sum equivalent to the compensation paid at level IV of the Federal Executive Salary Schedule, pursuant to section 5315 of title 5, prorated on a daily basis for each day spent in the work of the Commission, and shall be paid actual travel expenses, and per diem in lieu of subsistence expenses when away from his usual place of residence, in accordance with section 5 of the Administrative Expenses Act of 1946, as amended.

(b) Each member of the Commission who is otherwise in the service of the Government of the United States shall serve without compensation in addition to that received for such other service, but while engaged in the work of the Commission shall be paid actual travel expenses, and per diem in lieu of subsistence expenses when away from his

usual place of residence, in accordance with the provisions of the Travel Expenses Act of 1949, as amended.

(c) Members of the Commission shall be considered "special Government employees" within the meaning of section 202 (a) of title 18.

SEC. 303. DURATION OF COMMISSION.—The Commission shall exercise its powers and duties for a period of five years following the first appropriation of funds for its activities and the appointment and qualification of a majority of the members. It shall make a final report to the President and to the Congress on its activities as soon as possible after the expiration of the five-year period and shall cease to exist thirty days after the date on which its final report is submitted.

SEC. 304. POWERS AND DUTIES.—(a) For the purpose of carrying out its responsibilities under the Act, the Commission shall have authority—

(1) after consultation with representatives of criminal justice agencies subject to the Act, and after notice and hearings in accordance with the Administrative Procedures Act, to issue such regulations, interpretations, and procedures as it may deem necessary to effectuate the provisions of this Act, including regulations limiting the extent to which a Federal criminal justice agency may perform telecommunications or criminal

identification functions for State or local criminal justice agencies or include in its information storage facilities, criminal justice information, or personal identification information relative to violations of the laws of any State;

(2) to conduct hearings in accordance with section 305;

(3) to bring civil actions for declaratory judgments, cease-and-desist orders, and such other injunctive relief as may be appropriate against any agency or individual for violations of the Act or of its rules, regulations, interpretations or procedures;

(4) to make studies and gather data concerning the collection, maintenance, use, and dissemination of any information subject to the Act and compliance of criminal justice agencies and other agencies and individuals with the provisions of the Act;

(5) to require from each criminal justice agency information necessary to compile a directory of criminal justice information systems subject to the Act and publish annually a directory identifying all such systems and the nature, purpose, and scope of each;

(6) to conduct such audits and investigations as it may deem necessary to insure enforcement of the Act; and

(7) to delay the effective date of any provision of

this Act for up to one year, provided that such delay is necessary to prevent serious adverse effects on the administration of justice.

(b) The Commission shall report annually to the President and to the Congress with respect to compliance with the Act and concerning such recommendations as it may have for further legislation. It may submit to the President and Congress and to the chief executive of any State such interim reports and recommendations as it deems necessary.

SEC. 305. HEARINGS AND WITNESSES.—(a) The Commission, or, on authorization of the Commission, any three or more members, may hold such hearings and act at such times and places as necessary to carry out the provisions of this Act. Hearings shall be public except to the extent that the hearings or portions thereof are closed by the Commission in order to protect the privacy of individuals or the security of information protected by this Act.

(b) Each member of the Commission shall have the power and authority to administer oaths or take statements from witnesses under affirmation.

(c) A witness attending any session of the Commission shall be paid the same fees and mileage paid witnesses in the courts of the United States. Mileage payments shall be tendered to the witness upon service of a subpena issued on behalf of the Commission or any subcommittee thereof.

(d) Subpenas for the attendance and testimony of witnesses or the production of written or other matter, required by the Commission for the performance of its duties under this Act, may be issued in accordance with rules or procedures established by the Commission and may be served by any person designated by the Commission.

(e) In case of contumacy or refusal to obey a subpena any district court of the United States or the United States court of any territory or possession, within the jurisdiction of which the person subpenaed resides or is domiciled or transacts business, or has appointed an agent for the receipt of service or process, upon application of the Commission, shall have jurisdiction to issue to such person an order requiring such person to appear before the Commission or a subcommittee thereof, there to produce pertinent, relevant, and nonprivileged evidence if so ordered, or there to give testimony touching the matter under investigation; and any failure to obey such order of the court may be punished as contempt.

(f) Nothing in this Act prohibits a criminal justice agency from furnishing the Commission information required by it in the performance of its duties under this Act.

SEC. 306. DIRECTOR AND STAFF.—There shall be a full-time staff director for the Commission who shall be appointed by the President by and with the advice and consent

of the Senate and who shall receive compensation at the rate provided for level V of the Federal Executive Salary Schedule, pursuant to section 5316 of title 5. The President shall consult with the Commission before submitting the nomination of any person for appointment as staff director. Within the limitation of appropriations and in accordance with the civil service and classification laws, the Commission may appoint such other personnel as it deems advisable: *Provided, however,* That the number of professional personnel shall at no time exceed fifty. The Commission may procure services as authorized by section 3109 of title 5, but at rates for individuals not in excess of the daily equivalent paid for positions at the maximum rate for GS–18 of the General Schedule under section 5332 of title 5.

STATE INFORMATION SYSTEMS REGULATIONS

SEC. 307. (a) The Commission shall encourage each of the States to create or designate an agency to exercise statewide authority and responsibility for the enforcement within the State of the provisions of the Act and any related State statutes, and to issue rules, regulations, and procedures, not inconsistent with this Act or regulations issued pursuant to it, regulating the maintenance, use, and dissemination of criminal justice information within the State.

(b) Where such agencies are created or designated, the Commission shall rely upon such agencies to the maximum

extent possible for the enforcement of the Act within their respective States.

(c) Where any provision of this Act requires any criminal justice agency to establish procedures or issue rules or regulations, it shall be sufficient for such agencies to adopt or certify compliance with appropriate rules, regulations, or procedures issued by any agency created or designated pursuant to subsection (a) of this section or by any other agency within the State authorized to issue rules, regulations, or procedures of general application, provided such rules, regulations or procedures are in compliance with the Act.

CIVIL REMEDIES

SEC. 308. (a) Any person aggrieved by a violation of this Act or regulations promulgated thereunder shall have a civil action for damages or any other appropriate remedy against any person or agency responsible for such violation. An action alleging a violation of section 209 shall be available only after any administrative remedies established pursuant to that section have been exhausted.

(b) The Commission on Criminal Justice Information System shall have a civil action for declaratory judgments, cease-and-desist orders, and such other injunctive relief as may be appropriate against any criminal justice agency in order to enforce the provisions of the Act.

(c) If a defendant in an action brought under this sec-

tion is an officer or employee or agency of the United States the action shall be brought in an appropriate United States district court. If the defendant or defendants in an action brought under this section are private persons or officers or employees or agencies of a State or local government, the action may be brought in an appropriate United States district court or in any other court of competent jurisdiction. The district courts of the United States shall have jurisdiction over actions described in this section without regard to the amount in controversy.

(d) In any action brought pursuant to this Act, the court may in its discretion issue an order enjoining maintenance or dissemination of information in violation of this Act or correcting records of such information or may order any other appropriate remedy, except that in an action brought pursuant to subsection (b) the court may order only declaratory or injunctive relief.

(e) In an action brought pursuant to subsection (a), any person aggrieved by a violation of this Act shall be entitled to actual and general damages but not less than liquidated damages of $100 for each violation and reasonable attorneys' fees and other litigation costs reasonably incurred. Exemplary and punitive damages may be granted by the court in appropriate cases brought pursuant to subsection

(a). Any person or agency responsible for violations of this Act shall be jointly and severally liable to the person aggrieved for damages granted pursuant to this subsection: *Provided, however,* That good faith reliance by an agency or an official or employee of such agency upon the assurance of another agency or employee that information provided the former agency or employee is maintained or disseminated in compliance with the provisions of this Act or any regulations issued thereunder shall constitute a complete defense for the former agency or employee to a civil damage action brought under this section but shall not constitute a defense with respect to equitable relief.

(f) For the purposes of this Act the United States shall be deemed to have consented to suit and any agency of the United States found responsible for a violation shall be liable for damages, reasonable attorneys' fees, and litigation costs as provided in subsection (e) notwithstanding any provisions of the Federal Tort Claims Act.

(g) A determination by a court of a violation of internal operating procedures adopted pursuant to this Act should not be a basis for excluding evidence in a criminal case unless the violation is of constitutional dimension or is otherwise so serious as to call for the exercise of the supervisory authority of the court.

CRIMINAL PENALTIES

SEC. 309. Any Government employee who willfully disseminates, maintains, or uses information knowing such dissemination, maintenance, or use to be in violation of this Act shall be fined not more than $10,000.

AUDIT AND ACCESS TO RECORDS BY THE GENERAL ACCOUNTING OFFICE

SEC. 310. (a) The Comptroller General of the United States shall from time to time, at his own initiative or at the request of either House or any committee of the House of Representatives or the Senate or any joint committee of the two Houses, conduct audits and reviews of the activities of the Commission on Criminal Justice Information under this Act. For such purpose, the Comptroller General, or any of his duly authorized representatives, shall have access to and the right to examine all books, accounts, records, reports, files, and all other papers, things, and property of the Commission or any Federal or State agencies audited by the Commission pursuant to section 304(a)(6) of this Act, which, in the opinion of the Comptroller General, may be related or pertinent to his audits and reviews of the activities of the Commission. In the case of agencies audited by the Commission, the Comptroller General's right of access shall apply during the period of audit by the Commission and for three years thereafter.

(b) Notwithstanding any other provision of this Act, the Comptroller General's right of access to books, accounts, records, reports, and files pursuant to and for the purposes specified in subsection (a) shall include any information covered by this Act. However, no official or employee of the General Accounting Office shall disclose to any person or source outside of the General Accounting Office any such information in a manner or form which identifies directly or indirectly any individual who is the subject of such information.

PRECEDENCE OF STATE LAWS

SEC. 311. Any State law or regulation which places greater restrictions upon the maintenance, use, or dissemination of criminal justice information, criminal justice intelligence information, or criminal justice investigative information or which affords to any individuals, whether juveniles or adults, rights of privacy or other protections greater than those set forth in this Act shall take precedence over this Act or regulations issued pursuant to this Act with respect to any maintenance, use, or dissemination of information within that State.

APPROPRIATIONS AUTHORIZED

SEC. 312. For the purpose of carrying out the provisions of this Act, there are authorized to be appropriated such sums as the Congress deems necessary.

SEVERABILITY

SEC. 313. If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of the Act and the application of the provision to other persons not similarly situated or to other circumstances shall not be affected thereby.

REPEALERS

SEC. 314. The following provisions of law are hereby repealed:

(a) the second paragraph under the headings entitled "Federal Bureau of Investigation; Salaries and Expenses" contained in the Department of Justice Appropriations Act, 1973; and

(b) any of the provisions of the Privacy Act of 1974 (Public Law 93-579, 88 Stat. 1896), applicable to information covered by this Act.

EFFECTIVE DATE

SEC. 315. The provisions of sections 301 through 307 and of sections 310 and 312 of this Act shall take effect upon the date of enactment and members, officers, and employees of the Commission on Criminal Justice Information may be appointed and take office at any time after that date. Provisions of the remainder of the Act shall take effect one

year after the date of enactment: *Provided, however,* That the Commission may, in accordance with section 304(b), delay the effective date of any provision for up to one additional year.

## SECTION-BY-SECTION ANALYSIS

The Criminal Justice Information Control and Protection of Privacy Act of 1975 is designed to provide minimum national standards for the maintenance, use and dissemination of personal information by criminal justice agencies in order to ensure the security, accuracy and completeness of the information and to protect the rights of privacy of individuals who are the subjects of that information.

Section 101 contains the findings and states the basis for Congressional action. It recognizes the necessity of exchanges of information among criminal justice agencies, but notes the potential for infringement of individual rights if the information itself is inaccurate or incomplete, or is used or disseminated in an irresponsible manner. Acknowledging the primary role of the States, it nevertheless recognizes the interconnected role of Federal and State criminal justice information systems. It relies on the power of Congress to regulate interstate commerce in information and its power to impose restrictions on State and local criminal justice agencies receiving Federal funds or other benefits.

## DEFINITIONS

Section 102 defines some of the key terms used in the bill, although not all terms are specifically defined.

"The administration of criminal justice" is defined to include the whole range of functions concerned with crime, from protective measures to prevent the commission of crimes through the rehabilitation of convicted persons. The term also specifically includes the collection, storage or dissemination of criminal justice information.

"Criminal justice agency" includes police, prosecutors, courts and corrections as well as a number of auxiliary services performed by governmental agencies. It includes not only those governmental units, such as police departments or district attorneys' offices, whose major function is criminal justice but also subunits of governmental agencies which perform criminal justice functions. Thus, the Criminal Section of the Civil Rights Division of the U.S. Department of Justice, or an equivalent state agency, would be a "criminal justice agency." Similarly, the Antitrust Division of the Department of Justice or an Inspector General's Office which is conducting a criminal investigation in a particular case would be a "criminal justice agency" for purposes of that case even if its primary function is civil in nature. "Agency" is not used in any rigid sense. An organized crime strike force composed of members of various agencies would nevertheless be a "criminal justice agency" within the meaning of the bill.

The term also includes central data processing centers that process criminal justice information as well as other kinds of information. Thus, a central State data processing unit that provides services for criminal justice agencies as well as numerous non-criminal justice agencies in the State would be considered a criminal justice agency to the extent that it processes criminal justice information, although the processing of such information might constitute a relatively small part of its total activities.

"Criminal justice information" is the collective term for the following types of information which are defined separately—arrest record information, criminal record information, criminal history record information and correctional and release information. This definition is designed so that limited exchange of routine information reflecting the status of a criminal case and its history, or reports compiled for bail or probation, is not impaired as the information moves between government agencies.

The definitions of "criminal justice information," "criminal history information" and "arrest record information" should be read in conjunction with sections 103(c) and 203(h), which make it clear that the bill covers only filing systems indexed by name. It does not cover public records indexed by date, such as police blotters, incident reports or court records. The public, particularly members of the press, would still have access to such records and to other kinds of information that traditionally have been considered in the public domain.

"Arrest record information" is defined to include only that data on a typical "rap sheet" which indicates an arrest or initiation of charges but does not show the disposition of those charges. If a disposition is indicated, the information becomes "criminal history record information." If the disposition data indicates that the individual pleaded guilty or nolo contendere to criminal charges or was convicted of a criminal offense, the arrest and disposition data together constitute "conviction record information." This term also includes sentencing

information and information indicating that outcome of any appeal of a judgment entered after a plea or conviction. If the disposition indicates that the arrest was concluded other than by a judgment of conviction—that is, that criminal charges were not brought, that prosecution was not begun or was abandoned or was indefinitely postponed, that charges were dismissed or the individual was acquitted on any grounds, or that the criminal proceedings growing out of the arrest were otherwise terminated in the individual's favor—the information constitutes "nonconviction record information."

"Disposition" is defined to include all actions that terminate an arrest or any criminal proceedings growing out of the arrest. In addition to the dispositions mentioned in the preceding paragraph, the term includes any other actions, by whatever name that may be used in particular States, that terminate criminal proceedings at any stage beginning from the time of arrest. It is important to note that a single case may have more than one disposition, such as a conviction, followed by sentencing, followed by a reversal on appeal or by parole, pardon or executive clemency.

"Correctional and release information" is defined to include reports prepared on an individual at various stages of the criminal justice process from bail to parole. It includes pre-sentence reports, medical and psychiatric reports as well as the more typical correctional data.

"Criminal justice intelligence information" includes information collected to anticipate or monitor possible criminal activity as distinguished from the investigation of specific criminal acts which have already occurred.

"Criminal justice investigative information" is that data compiled in determining who committed a specific crime and compiling evidence to prove guilt.

## APPLICABILITY

Section 103 sets forth the coverage of the bill. Subsection (a) specifies that all Federal criminal justice agencies are covered, as are those State or local agencies which are funded in whole or in part by the Federal government. In addition, criminal justice agencies exchanging interstate information with Federal agencies, with federally-funded State or local agencies, or on an interstate basis are covered. In the latter case, the bill applies only to the extent of the exchange. Thus, a police department which maintains numerous records of its own and also exchanges some information with the FBI must comply with the bill in the handling of information sent to the FBI or received from it, but is not obligated to comply with the bill with respect to information which it collects and uses solely within the department without Federal funding or support.

Subsection (b) requires that information originally obtained from a foreign government or international agency and included with information subject to the bill be handled in the same manner as information generated within the United States. The bill does not prohibit exchanges of criminal justice information with foreign governments or international organizations, either pursuant to treaties or agreements or on an ad hoc basis. It requires, however, that the agency in the United States undertake to insure to the maximum extent feasible that the foreign agency receiving the information uses it in a manner consistent with the principles of the bill.

Subsection (c) excludes certain types of information from the application of the bill. Public information such as court opinions, court proceedings and police blotters remain public and are not subject to the restrictions in the bill. Motor vehicle or pilot license registries which are maintained for licensing purposes by departments of transportation, motor vehicles or similar licensing agencies are not subject to the restrictions in the bill. However, records of serious traffic offenses such as manslaughter or drunk driving, which are maintained by criminal justice agencies, remain subject to the bill.

Military justice records remaining in the Department of Defense are exempt from the bill but if "absent without leave" or other military justice information is transferred to a Federal or State agency other than the Defense Department, it becomes subject to the bill. Similarly, criminal justice information exchanged with the Department of Defense is subject to the bill.

Statistical and analytical reports, such as the Uniform Crime Statistics, are not subject to the bill since individual offenders are not identified.

## TITLE II

Title II of the bill specifies the basic restrictions on the maintenance, dissemination and use of criminal justice information and imposes certain obligations on criminal justice agencies.

Section 201 sets general restrictions on access to and use or dissemination of criminal justice information within the criminal justice community.

Generally, conviction records may be exchanged freely by criminal justice agencies. Correction and release information can be disseminated only to other criminal justice agencies or to the subject if permitted by statute or court order.

Raw arrest records and criminal history records which terminated in the defendant's favor may be disseminated to another criminal justice agency only where the individual has applied for a job at that agency, the individual's case has been referred to that agency for adjudication or the individual has been referred to the agency for supervision. Such records could also be made available on a relatively routine basis to law enforcement agencies once the agency had already arrested the individual in question. These records should be made available only on a very limited basis to law enforcement agencies prior to arrest when the information will be used to develop investigative leads and the officer can point to "specific and articulable facts which taken together with rational inferences from those facts warrant the conclusion that the individual has committed or is about to commit a criminal act and that the information would be relevant to the act."

The information should be available only on a "need-to-know", "right-to-know" basis. This means that the agency receiving the information has established procedures designed to assure that the person receiving the information has demonstrated that he is a detective or patrolman performing detective functions and that he needs the information for a particular case.

The "specific and articulable facts" standard derives from the Supreme Court opinion in the case of *Terry* v. *Ohio*, 392 U.S. 1 (1968), in which the court permitted stop and frisk on such grounds. Based on the *Terry* language, in evaluating the reasonableness of a request for records for investigative purposes, "due weight must be given, not to (the officer's) inchoate and unparticularized suspicion or 'hunch' but to the specific reasonable inference which he is entitled to draw from the facts in light of his experience." 392 U.S. 27. In using the identical language, it is intended that an investigating officer should be able to justify requests for information with similar specificity.

The section also permits arrest records and nonconviction records to be made available to a law enforcement officer where the information might alert him of a danger to his life, or for "similar essential purposes." It is intended that where information is used for these purposes, its utility clearly outweighs any risk to the rights of the subject of the information. Such circumstances should be set out in agency procedures.

Criminal justice agencies must establish operating procedures "reasonably designed" to insure that the use and dissemination of arrest records and nonconviction records are restricted to the purposes authorized by this section. Where such information is obtained from another criminal justice agency, section 207(a)(3) requires that records of that exchange (either written or on computer tape) must be maintained for three years. Periodic audit of these records is required to ensure that the information is not being disseminated or used improperly. While it was not considered feasible to require a similar audit trail for arrest records used within the agency maintaining them, the agency is under an obligation to adopt some affirmative measures, such as training programs, directives, or other appropriate procedures which are designed to prevent abuse.

## WANTED PERSONS AND IDENTIFICATION INFORMATION

Section 202 permits the use and dissemination of wanted person information and identification information for any authorized criminal justice purpose. Thus, wanted posters may be published and posted, mug shots may be shown to potential witnesses, and fingerprints may be used to identify crash victims. However, a fingerprint card which contains arrest record information may be used or disseminated only under the same procedures as other arrest record information. The section also provides that the use of automated fugitive or stolen property files, such as those maintained by the NCIC, is not restricted by the limitations on direct access to criminal justice information contained in other parts of the bill.

Section 203 sets forth policies for the dissemination and use of criminal justice information outside of the criminal justice system for such purposes as employment, licensing or credit ratings. Except for uses specifically authorized in the section or in other parts of the bill, only conviction records and certain arrest records may be made available for non-criminal justice purposes and then only if the specific purpose is expressly authorized by Federal or state law.

To satisfy the "expressly authorized" requirement, the statute must specifically deny employment, licensing on other civil rights or privileges to persons convicted of a crime or must require a criminal record check prior to employment, licensing or the like. The statute must refer explicitly to criminal conduct. Statutes which contain requirements or exclusions based on "good moral character" or "trustworthiness" or similar nonspecific bases would not be sufficient to authorize dissemination. The information released must be relevant to the authorized purpose and must be used only for that purpose. Thus, an arrest record obtained for employment screening could not be used to deny the individual a license or to revoke a license. The information may not be copied or retained by the recipient beyond the time necessary to accomplish the purpose for which it was made available. For example, where information is released for a statutorily authorized preemployment investigation, the information must be destroyed or returned to the criminal justice agency from which it was received as soon as the initial employment decision is made. Should the information be required at a later time, it can be obtained by a new request to a criminal justice agency.

In all cases where information is requested pursuant to the above procedure, the requestor must notify the individual to whom the information relates that the information will be requested and that he has the right to review the information (pursuant to section 209) prior to its dissemination to ensure that it is complete and accurate. Individual notice in each instance is not required so long as the employment application form or license application form itself indicates that this type of information may be requested concerning the individual. Agencies which have authority to make continuing checks on the records of their employees or others must find some mechanism, such as an employee bulletin, to ensure that all those whose records may be obtained are made aware of that fact.

Nonconviction record information may not be made available pursuant to the general authorization discussed above. Arrest records may be made available only if the individual was formally charged and no more than a year has passed since charges were brought and if prosecution of the charge is still pending. Thus, before an arrest record without a disposition may be released for a noncriminal justice purpose, the criminal justice agency must have some affirmative indication that the charge is still pending.

Subsection (d) permits criminal justice information to be made available to qualified persons for research. A limited amount of discretion is provided the criminal justice agency in determining whether the individual seeking access does so with the good faith intent of using the information for research purposes. It is intended that the types of individuals permitted access be rather liberally construed as long as the applicant intends to seek statistical rather than individually identifiable information. As long as the individual has a research plan which relies upon such statistical information it is not the responsibility of the criminal justice agency to pass upon the qualifications of the individual to do the research or validity of the research design. It is assumed that this provision will be invoked mostly by scholars and students of the criminal justice system including investigative reporters from both the print and electronic media.

Section 203(e) contains a specific statutory authorization for the Immigration and Naturalization Service and the Department of State to obtain the criminal justice information about individuals that is necessary to enforce the immigration laws. However, they must adopt specific procedures to ensure that arrest record information is used as an investigative lead, and that any adverse decision based on arrest record information is reviewed at a supervisory level before a final decision is made. The agency's own procedures would specify the appropriate level of review.

A similar statutory authorization is provided in subsection (f) for the Treasury Department's Bureau of Alcohol, Tobacco and Firearms, Customs Service, Internal Revenue Service, and Office of Foreign Assets Control which have mixed civil and criminal functions and have specialized needs for criminal justice information in order to carry out their statutory duties. Again, the Treasury Department is required to adopt procedures to prevent the abuse of arrest record information.

The Drug Enforcement Administration of the U.S. Department of Justice would be authorized by subsection (g) to disseminate criminal record information (but not arrest record information) to registered drug manufacturers for purposes of enforcing the Controlled Substances Administration Act. The manufacturers themselves are not authorized to obtain the information from any other source except public records.

Announcement of arrest, convictions and similar stages of the criminal justice process to the press is allowed under subsection (h) as are announcements of the correctional status of an individual, e.g., on furlough, on parole, etc., and new developments in the course of an investigation. These announcements must be related, however, to events that are on-going, rather than to past history. Thus, the announcement of an arrest should be made within a few days of its occurrence, not five years later. While past criminal history is not to be volunteered to the public, it is permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. If the press, or any member of the public should inquire directly, "Was Joe Smith arrested by your Department on July 15, 1941?" and that fact can be ascertained from a police blotter or similar record of entry, a criminal justice agency may confirm it.

Section 204 authorizes the dissemination of criminal justice information for certain employment purposes. Subsection (a) provides that such information may be provided to the nominating, confirming or appointing authority of Federal, State or local governments in connection with the appointment of criminal justice agency executives, judges, or members of the Commission on Criminal Justice Information which would be established by the bill or similar state boards. In all cases, a written consent by the individual to be considered for the position and to have criminal justice information obtained in connection therewith is required.

Subsection (b) is the specific statutory authorization for access to criminal justice information in connection with Federal employment and security clearances. Since this section permits access to raw arrests without the subject's consent, it is intended that it be narrowly construed so that such information would be available only for "full field background investigations" similar to those conducted pursuant to section 3(b) of Executive Order 10450 on "Security Requirements for Government Employment" and described in greater detail in Chapter 736, Subchapter 2, Section 2-5 of the Federal Personnel Manual.

For employment investigations only unsealed arrest records and criminal history records may be made available. Sealed records may be made available for security clearance investigations, and for "top secret" security clearances investigative and intelligence information may also be made available. In every case, the individual must be put on notice at the time he is employed or otherwise takes action that initiates a background investigation that access to this type of information will be sought.

Subsection (c) prohibits agencies or persons who lawfully gain access to information from using the information for an improper purpose or from disseminating the information in a manner not permitted by the legislation.

Section 205 prohibits anyone who obtains criminal justice information from further disseminating it to unauthorized persons. Thus, the pharmacists licensing board which has statutory authority to obtain criminal justice information may not pass that information on to a barber's licensing board that does not have similar statute. An exception is made to permit rehabilitation officials to summarize criminal record information or correctional and release information for a prospective employer or others if this will assist the subject of the record and he consents. For example, a parole official assisting a convict about to be released in securing employment may summarize the convict's prison record to a prospective employer in order to help obtain employment. The record itself may not be disseminated, however.

Section 206 is based on a provision contained in Project SEARCH's model state statute and the Massachusetts arrest records statute. It places limitations on access to criminal justice information via categories other than name. With limited exceptions, inquiries must be based on identification of a specific individual rather than on other types of information classification such as crime characteristics or offender characteristics. For investigation purposes prior to the arrest of an individual, inquiries should be based upon individual names and other personal identifiers. After arrest, the inquiry must be based upon positive identification by fingerprints or the like. Subsection (b) requires agencies to adopt special procedures governing access to a criminal justice data bank by offense—i.e., a print-out on all persons charged with first degree burglary with certain physical descriptions or with a certain modus operandi and from a certain geographical area.

Although few criminal justice data banks have this capability, grave risks are seen to the rights of data subjects if the computer is used routinely as a substitute for the experienced and cautious detective. Obviously, permitting unbridled access to computer printouts of names of individuals based on racial characteristics, geographical area or crime (e.g., persons arrested for engaging in unlawful demon-

strations) would present grave policy and constitutional questions. Agency procedures must limit such inquiries to the investigation of particular criminal offenses and must limit dissemination of the information to those persons who need it for the performance of investigative duties.

Section 207 requires every agency covered by the Act to promulgate regulations on security, accuracy and updating and sets out in general terms what those regulations must provide. Each criminal justice agency must maintain for a period of three years a complete record, or audit trail, of the individuals who have access to its information and the purposes for which the information is requested. Subsection (b) allows the Commission created by Title III of the Act to suspend the provisions of this section as they relate to information collected prior to the effective date of the Act when the Commission determines that full implementation of this section is infeasible because of costs or other compelling factors. It is intended that the Commission explore all other alternatives before actually suspending a provision for old records. Therefore, it is intended that the provisions of this section might be more loosely construed with regard to old records than with new records. This approach is preferable to actual suspension of the provisions. For example, it might be argued that it would be too burdensome to require the FBI's Identification Division to go back and add "the nature, purpose and disposition" of all past requests in an effort to reconstruct audit trails for old records. In many cases the identity of the requestor might be sufficient to indicate "the nature, purpose and disposition" of the request.

Obviously, some state licensing agencies could only request a rap sheet for one purpose, and if the agency's name appears on the audit trail, then the FBI could assume that the request was for that purpose. Rather than actually suspend the application of this subsection to old rap sheets, it would be preferable for the Commission to allow some flexibility in applying these provisions to old files.

Section 208 requires every agency or information system covered by the act to promulgate regulations on sealing or purging of information. Such regulations or procedures must provide for sealing or purging of information where required by a Federal or a State statute other than this Act or by Federal or State court order. Furthermore, the section requires that each agency promptly seal certain old conviction records unless a class of offenses are exempted by state or Federal law. It is intended that sealing a record might be accomplished by moving a record from a routinely available status to a status requiring a special procedure to gain access. In manual systems this might mean moving a record from open filing drawers to microfilm while in automated systems a record might be considered sealed by moving the information from on-line to off-line. An index of sealed records may be maintained but access to the index would be limited to law enforcement employees. Records can be unsealed by court order or automatically in certain circumstances, such as where the individual requests review pursuant to section 209 or where special access is permitted pursuant to section 204 in screening security clearances.

Section 209 requires every agency covered by the Act to establish the means for an individual to have access to his or her own arrest record information or criminal history record information and to challenge inaccurate or incomplete information contained therein. The section sets out what regulations to this end must provide. This section should be read along with Section 308, which provides court review procedures where the agency fails to comply with Section 209 or any other provision of the Act.

Sections 210 and 211 place limitations on the dissemination of criminal justice intelligence information (Section 210) and criminal justice investigative information (Section 211). As a general rule such information would be exchanged between criminal justice agencies only where a "need to know" and "right to know" had been demonstrated by the requesting agency and by officers and employees within the agency (See subsection 210(b) and 211(c)). "Need to know" and "right to know" means that the agency making the request must establish that it is conducting an investigation as part of its responsibilities in the administration of criminal justice and that it has good reason for needing the information for the investigation. Within the agency only those employees conducting the investigation or their superiors would have access to the incoming intelligence or investigative information.

Section 210 also provides that intelligence information should be collected on individuals only if there are grounds existing connecting that person with known or suspected criminal activity. It also provides for routine review of files to determine whether such grounds continue to exist (Subsection 210(b)). The same section also provides that intelligence information on an individual may be dis-

seminated to a second agency only if that agency is able to point to "specific and articulable facts which, taken together with rational inferences from those facts, warrant the conclusion that the individual has committed or is about to commit a criminal act and that the information may be relevant to that act." (Subsection 210(d)). This language, similar to that contained in Section 201, is based on the *Terry* case, and it is intended that it be interpreted in the same manner.

The section prohibits the entry of criminal justice investigative or intelligence information in an information system which maintains criminal history information. However, this should not be construed to prohibit the inclusion of criminal history information in intelligence or investigative files. Although investigative and intelligence information may be automated, remote access to such automated systems is generally prohibited.

However, the bill would permit the maintenance of an index to intelligence files which could be accessed by remote terminal from outside the agency. The index might maintain the name, identification record information, criminal history record information and other public record information on individuals upon whom more complete intelligence files exist. The requesting agency's request could be referred automatically via the index to another criminal justice agency possessing more complete information on the individual in question. It is intended that this index be operated in such a manner that it not undermine subsections (b), (c) and (d) of section 210 which provide the maintaining agency with a right to review all requests for access to its intelligence files. Therefore, such an index must be designed so that a requesting agency is not automatically informed of the existence of a file or the name of the maintaining agency but that the maintaining agency might be immediately and automatically informed of the request so that it can in its discretion respond to the requesting agency if it determines that the requirements of subsections (b), (c) and (d) have been met.

Section 211 also contains a provision permitting an individual to see his own investigative file where such disclosure is permitted under the Freedom of Information Act and other statutes or court rules. This provision would continue the practice of discovery in criminal cases in both the Federal and State courts. For example, section 3500 of title 18 of the United States Code, the so-called "Jencks Act" permits disclosure to a defendant of prior statements by witnesses to the police. Section 211 would not affect that type of disclosure.

Although intelligence and investigative information is generally restricted to criminal justice agencies, a limited exception is permitted for intelligence "assessments." It is understood that an intelligence assessment is a summary provided to a government official about the impact which certain intelligence information will have upon the operations of the official's agency or as an aid to making official decisions within his authority. Intelligence files are not made available in the course of such an assessment but only a summary of the contents of such file. The exceptions to the general prohibitions embodied in the "assessment" role are to be narrowly construed. Information should be made available to private persons only where there is imminent danger to their life or property. Also intelligence and investigative information would be available to noncriminal justice agencies pursuant to Section 204.

## TITLE III

### Administrative Provisions; Regulations, Civil Remedies; Criminal Penalties

#### COMMISSION ON CRIMINAL JUSTICE INFORMATION

Title III establishes the administrative and enforcement mechanisms for the bill.

Section 301 creates a cooperative Federal-State administrative structure for enforcement of the Act. A Commission on Criminal Justice Information is established as an independent agency with the responsibility for administration and enforcement of the Act. The commission would be composed of thirteen members. The membership should reflect the varying attitudes of all segments of the criminal justice community: Federal law enforcement, State law enforcement, the judiciary, corrections, and the private sector that deals directly in this area. The Attorney General automatically becomes a member with two other Federal representatives designated by the President. The other designated member will be on the recommendation of the Judicial Conference of the United States. However, because of the traditional reluctance of members of the judiciary to participate in such arrangements—perhaps because of separation of powers concerns—the appoint-

ment of the thirteenth member is made discretionary with the Judicial Conference. The representative of the United States Judicial Conference would serve at the pleasure of the Conference.

Seven of the appointed members will represent state criminal justice agencies, a state criminal justice agency to be defined broadly so that serious attempts will be made to select some people who are other than law enforcement officials. The chairman will be designated from amongst these seven appointees. The two remaining appointed members will be private citizens well versed in privacy, computer technology and constitutional law.

Section 302 provides the guidelines for the compensation of the members of the Commission.

Section 303 was drafted to allay the concerns of many that this legislation would establish a ponderous bureaucracy that would become entrenched with time. This section provides a legislative life of five years for the Commission on Criminal Justice Information. So that the time that is legislatively given to the Commission is not circumvented, the time is not considered to run until at least a majority of the members have been appointed and qualified. This section also requires the Commission to report to the President and Congress upon its termination. This allows Congress to evaluate the work of the Commission to determine whether the Commission accomplished the goal of establishing the guiding precedent for future administration of criminal justice information systems. At that point the Congress would have the alternative of passing the regulation and control of criminal justice information systems to the Attorney General or extending the life of the Commission.

Section 304 sets out the powers and the duties of the Commission on Criminal Justice Information. Among its powers is the authority to issue general regulations in enforcement of the letter and spirit of the Act. This action would follow consultation with representatives of criminal justice agencies which are subject to the Act and after notice and hearings pursuant to the Administrative procedures Act. The power to regulate includes limiting the extent to which a Federal criminal justice agency may perform telecommunications or criminal identification functions for state or local criminal justice agencies or include in its information storage facilities criminal justice information or personal identification information relative to violations of the laws of any state.

This means that the Commission would have authority to determine the extent to which the national criminal justice information system could operate its own telecommunications system or rely upon existing systems such as the National Law Enforcement Telecommunications System (NLETS). There has been concern about recent suggestions that the Justice Department has authorized the Federal Bureau of Investigation to establish its own telecommunications system within the National Crime Information System. It would be preferred that existing state-based organizations such as NLETS be relied upon in the operation of a national criminal justice information system because an overconcentration of powers and responsibility in the Federal government for telecommunications would be unhealthy and might be an inappropriate encroachment upon state and local law enforcement. In respect to the concept of a federally chartered corporation and Board control of the telecommunications system the Committee shares the view of Richard Velde of LEAA:

"* * * with respect to NLETS and any future developments that might occur, as far as an expanded telecommunications network for State and local criminal justice, as I indicated in my prepared testimony, we believe that the Project SEARCH model, of a policy board with an executive committee, much the same as is suggested in the chairman's bill, would be a very appropriate vehicle for policy determinations and regulation of this kind of system.

"There is a danger, when any single agency, be it Federal, State, or local, has policy control over a network of this kind. We think the responsibility should be shared."

All of Title III, in particular the creation of the Commission and its authority over a national criminal justice information system and the telecommunications question is viewed as a mechanism for sharing decision-making on these issues among local, state and Federal agencies.

The Commission is further authorized to conduct hearings and compel the attendance of witnesses in accordance with Section 305. The Commission would have the power to enforce its subpoena in Federal Court. It could bring civil action for any injunctive relief as may be appropriate. It will also have the authority to conduct studies on any segment of the operation of criminal justice information systems and its compliance with the Act. Such studies might conclude

with recommendations to the Congress for additional legislation. The Commission, further, has the authority to conduct audits and investigations it deems necessary to ensure enforcement of the Act. Most importantly, the Commission may delay the effective date of any portion of this Act on a selective basis up to one year. This delay can be based on any determination of the Commission of administrative necessity to financial necessity.

The duty of the Commission is one of an annual reporting requirement to the President and the Congress. It may issue any interim report as it deems necessary.

Section 305 provides the ground rules for the hearing process, including the issuance of subpoenas, the calling of witnesses, and the reimbursement of witnesses.

Section 306 provides for the staffing of the Commission on Criminal Justice Information. The director will be appointed by the President after consultation with the Commission. Other employees are subject to civil service qualifications. It should be noted that in an attempt to prevent the uncontrolled bureaucratic expansion of this new commission, the number of professional personnel is not to exceed fifty.

Section 307 encourages the states to create or designate an agency or office within their jurisdictions to exercise statewide responsibility for the enforcement of the Act. The Commission is expected to rely upon the determinations of such a state agency to the maximum extent possible.

Section 308 provides the judicial machinery for the exercise of the rights granted in Section 209 and elsewhere in the Act. The aggrieved individual may obtain both injunctive relief and damages, $100 recovery for each violation, actual and general damages, attorneys' fees, and other litigation costs whether violations were willful or negligent. An "aggrieved individual" covers an individual upon whom information is maintained, or used in violation of this Act or who is denied access to information to which he is entitled pursuant to any section of this Act. An "aggrieved individual" might also be a person denied information in violation of subsection 209(e). It does not require that the individual have suffered some further harm from the violation, such as loss of job or benefit, in order to have a cause of action. It is intended that the Commission may in its discretion intervene in any case in which it is not already a party and use in such litigation the results of any audit it might have conducted pursuant to Section 304.

New provisions have been added to the civil remedies section which would limit unnecessary interference by litigants with legitimate law enforcement activities. First, the section now provides an employee of a criminal justice agency or information system or the agency or information system with a complete defense to a damage action when he relies in good faith upon the representation of another agency or employee that information it disseminates is being handled in compliance with the Act. This provision would avoid the imposition of liability in circumstances where it would be impossible for an agency to recognize that information it receives or maintains is not in conformity with the Act. For example, it would exculpate a telecommunications system such as the National Law Enforcement Telecommunications System from liability for information it transmits in violation of the Act. Liability in that circumstance should fall on the agency which enters the information in the telecommunications system.

Second, the section would provide that a mere violation of this section could not be the basis for a motion to suppress evidence in a criminal proceeding. Of course, the provision does not limit the court's general supervisory authority to suppress evidence in circumstances of gross violation or in circumstances where the violation is of constitutional dimensions.

Section 309 provides criminal penalties for willful violations of the Act. (No prison penalty is provided.)

Section 310 provides authority for the Comptroller General to conduct certain audits and studies of the operations of the Commission on behalf of the Congress. In a letter to the Senate Subcommittee requesting inclusion of this provision the Comptroller General stated that although he thought the General Accounting Office's general statutory authority should be included in this legislation "because of the sensitive nature of the data involved." The Comptroller General also stated:

"While we fully support the intention of both bills that the administering executive agencies should be primarily responsible for properly managing the provisions of the bills, we also believe it is important that a specific provision be included in the bill providing the means for an independent congressional assessment of executive agencies' actions. In this way the Congress can have better assurance that the detailed audit by the executive agencies are adequate."

A provision almost identical to that proposed by the Comptroller General has been included.

Section 311 provides that any state statute or state regulation which imposes stricter privacy requirements on the operation of criminal justice data banks or upon the exchange of information covered by this Act takes precedence over this Act or any regulations issued pursuant to Section 304. The Commission would make the administrative decision as to which statute or regulation governs, and whether a regulation comports with this Act.

Section 312 authorized the appropriation of such funds as the Congress deems necessary for the purposes of the Act.

Section 313 is a standard severability provision.

Section 314 repeals a temporary authority for the Federal Bureau of Investigation to disseminate rap sheets to non-criminal justice agencies. It also repeals the Privacy Act of 1974 insofar as that Act relates to criminal justice information.

Section 315 makes most of the substantive provisions of the Act effective one year after its enactment, except that the Commission can suspend the application of any provisions of the Act for up to one additional year. The Commission is authorized to order such further suspensions on a provision-by-provision basis where it deems it applicable.

94TH CONGRESS
1ST SESSION

# S. 1427

IN THE SENATE OF THE UNITED STATES

APRIL 14, 1975

Mr. TUNNEY introduced the following bill; which was read twice and referred to the Committee on the Judiciary

# A BILL

To protect the constitutional rights and privacy of individuals upon whom criminal justice information, criminal justice investigative information, and criminal justice intelligence information have been collected and to control the collection and dissemination of criminal justice information, criminal justice investigative information, and criminal justice intelligence information, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,* That this Act may be cited as the "Criminal Justice Information Control and Protection of Privacy Act of 1975".

## TITLE I—FINDINGS AND DECLARATION OF POLICY; DEFINITIONS; APPLICABILITY

### CONGRESSIONAL FINDINGS AND DECLARATION OF POLICY

SEC. 101. The Congress finds and declares that the several States and the United States have established criminal justice information systems, criminal justice investigative information systems, and criminal justice intelligence information systems which have the capability of transmitting and exchanging criminal justice information, criminal justice investigative information, and criminal justice intelligence information between or among each of the several States and the United States; that the exchange of this information by Federal agencies is not clearly authorized by existing law; that the exchange of this information has great potential for increasing the capability of criminal justice agencies to prevent and control crime; that the exchange of inaccurate or incomplete records of such information can do irreparable injury to the American citizens who are the subjects of the records of the information; that the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from misuse of these systems; that citizens' opportunities to secure employment and credit and their right to due process, privacy, and other legal protections are endangered by misuse of these systems; that in order to secure the constitutional rights guaranteed by

the first amendment, fourth amendment, fifth amendment, sixth amendment, ninth amendment, and fourteenth amendment, uniform Federal legislation is necessary to govern these systems; that these systems are federally funded, that they contain information obtained from Federal sources or by means of Federal funds, or are otherwise supported by the Federal Government; that they utilize interstate facilities of communication and otherwise affect commerce between the States; that the great diversity of statutes, rules, and regulations among the State and Federal systems require uniform Federal legislation; and that in order to insure the security of criminal justice information systems, criminal justice investigative information systems, and criminal justice intelligence information systems, and to protect the privacy of individuals named in such systems, it is necessary and proper for the Congress to regulate the exchange of such information.

DEFINITIONS

SEC. 102. For the purposes of this Act—

(1) "Information system" means a system, whether automated or manual, operated or leased by Federal, regional, State, or local government or governments, including the equipment, facilities, procedures, agreements, and organizations thereof for the collection, processing, preservation, or dissemination of information.

(2) "Criminal justice information system" means an information system which contains only criminal justice information.

(3) "Criminal justice investigative information system" means an information system which contains criminal justice investigative information.

(4) "Criminal justice intelligence information system" means an information system which contains criminal justice intelligence information.

(5) "Automated system" means an information system that utilizes electronic computers, central information storage facilities, telecommunications lines, or other automatic data processing equipment used wholly or in part for data dissemination, collection, analysis, or display as distinguished from a system in which such activities are performed manually.

(6) "Dissemination" means the transmission of information, whether orally, in writing, or by electronic means.

(7) "The administration of criminal justice" means any activity by a criminal justice agency directly involving the apprehension, detention, pretrial release, posttrial release, prosecution, defense, adjudication, or rehabilitation of accused persons or criminal offenders or the collection, storage, dissemination, or usage of criminal justice information.

(8) "Criminal justice agency" means a court and any

other governmental agency created by statute or any subunit thereof created pursuant to statute, or State or Federal constitution which performs as its principal function, as authorized pursuant to statute, the administration of criminal justice, and any other agency or subunit thereof which performs a function which is the administration of criminal justice but only to the extent that it performs that function. A criminal justice agency also includes an organization which by contract with a criminal justice agency performs a function which is the administration of criminal justice but only to the extent that it performs that function. Any provision of this Act which relates to the activities of a criminal justice agency also relates to any information system under its management control or any such system which disseminates information to or collects information from that agency.

(9) "Criminal justice information" means identification record information, wanted persons record information, arrest record information, nonconviction record information, conviction record information, criminal history record information, and correctional and release information. The term does not include—

(A) statistical or analytical records or reports in which individuals are not identified and from which their identities are not ascertainable,

(B) criminal justice investigative information,

(C) criminal justice intelligence information, or

(D) records of traffic offenses maintained by departments of transportation, motor vehicles, or the equivalent, for the purpose of regulating the issuance, suspension, revocation, or renewal of drivers' licenses.

(10) "Identification record information" means fingerprint classifications, voice prints, photographs, and other physical descriptive data concerning an individual which does not include any indication or suggestion that the individual has at any time been suspected of or charged with a criminal offense.

(11) "Wanted persons record information" means identification record information on an individual against whom there is an outstanding arrest warrant including the charge for which the warrant was issued and information relevant to the individual's danger to the community and such other information that would facilitate the regaining of the custody of the individual.

(12) "Arrest record information" means notations of arrest, detention, indictment, filing of information, or other formal criminal charge on an individual which does not include the disposition arising out of that arrest, detention, indictment, information, or charge. The term shall not include an original book of entry or police blotter whether automated or manual maintained by a law enforcement

agency at the place of original arrest or detention, not indexed or accessible by name and required to be made public nor shall it include court records of public criminal proceedings or any index thereto indexed or accessible by date or by docket or file number or indexed or accessible by name so long as such index contains no other information than a cross-reference to the original court records by docket or file number.

(13) "Nonconviction record information" means criminal history record information which is not conviction record information.

(14) "Conviction record information" means criminal history record information disclosing that a person has pleaded guilty or nolo contendere to or was convicted of any criminal offense in a court of justice, sentencing information, and whether such plea or judgment has been modified or reversed.

(15) "Criminal history record information" means information on an individual consisting of notations of arrests, dententions, indictments, informations, or other formal criminal charges and any disposition arising from those arrests, detentions, indictments, informations, or charges. The term shall not include an original book of entry or police blotter whether automated or manual maintained by a law enforcement agency at the place of original arrest or place of

detention, not indexed or accessible by name and required to be made public nor shall it include court records of public criminal proceedings or official records of pardons or paroles or any index thereto indexed or accessible by date or by docket or file number or indexed or accessible by name so long as such index contains no other information than a cross-reference to the original court pardon or parole records by docket or file number.

(16) "Disposition" means information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the nature of the termination in the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Dispositions shall include, but not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, deceased, deferred disposition, dismissed-civil action, extradited, found insane, found mentally incompetent, pardoned, proba-

tion before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged, or executive clemency.

(17) "Correctional and release information" means information on an individual compiled by a criminal justice or noncriminal justice agency in connection with bail, pretrial or posttrial release proceedings, reports on the physical or mental condition of an alleged offender, reports on presentence investigations, report on inmates in correctional institutions or participants in rehabilitation programs, and probation and parole reports.

(18) "Criminal justice investigative information" means information associated with an identifiable individual compiled by a criminal justice agency in the course of conducting a criminal investigation of a specific criminal act including information pertaining to that criminal act derived from reports of informants and investigators, or from any type of surveillance. The term does not include criminal justice information nor does it include initial reports filed by a law enforcement agency describing a specific incident, not indexed or accessible by name and expressly required by State or Federal statute to be made public.

(19) "Criminal justice intelligence information" means information associated with an identifiable individual compiled by a criminal justice agency in the course of conducting an investigation of an individual relating to possible future



56-833 O - 75 - 5

criminal activity of an individual or relating to the reliability of such information including information derived from reports of informants, investigators, or from any type of surveillance. The term does not include criminal justice information nor does it include initial reports filed by a law enforcement agency describing a specific incident, not indexed or accessible by name and expressly required by State or Federal statute to be made public.

(20) "Law enforcement agency" means a criminal justice agency which is empowered by State or Federal law to make arrests for violations of State or Federal law.

(21) "Seal" means to close a record possessed by a criminal justice agency so that the information contained in the record is available only in the circumstances set out in section 208 (b) (5).

(22) "Judge of competent jurisdiction" means (a) a judge of a United States district court or a United States court of appeals; (b) a Justice of the Supreme Court of the United States; (c) a judge of any court of general criminal jurisdiction in a State; or (d) any other official in a State who is authorized by a statute of that State to enter orders authorizing access to criminal justice information.

(23) "Attorney General" means the Attorney General of the United States.

(24) "State" means any State of the United States, the

District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

APPLICABILITY

SEC. 103. (a) This Act applies to criminal justice information, criminal justice investigative information, or criminal justice intelligence information maintained in information systems which are—

(1) operated by the Federal Government,

(2) operated by a State or local government and funded in whole or in part by the Federal Government,

(3) operated as interstate systems,

(4) operated by a State or local government and engaged in the exchange of information with a system covered by paragraph (1), (2), or (3) but only to the extent such information is available for exchange or dissemination with a system covered by paragraph (1), (2), or (3).

(b) The provisions of this Act do not apply to—

(1) original books of entry or police blotters, whether automated or manual, maintained by a law enforcement agency at the place of original arrest or place of detention, not indexed or accessible by name and required to be made public;

(2) court records of public criminal proceedings or official records of pardons or paroles or any index thereto indexed or accessible by date or by docket or file num-

ber or indexed or accessible by name so long as such index contains no other information than a cross reference to the original pardon or parole records by docket or file number;

(3) public criminal proceedings and court opinions, including published compilations thereof;

(4) records or traffic offenses maintained by departments of transportation, motor vehicles, or the equivalent, for the purpose of regulating the issuance, suspension, revocation, or renewal or drivers' licenses;

(5) records relating to violations of the Uniform Code of Military Justice but only so long as those records are maintained solely with the Department of Defense; or

(6) statistical or analytical records or reports in which individuals are not identified and from which their identities are not ascertainable.

## TITLE II—COLLECTION AND DISSEMINATION OF CRIMINAL JUSTICE INFORMATION, CRIMINAL JUSTICE INVESTIGATIVE INFORMATION AND CRIMINAL JUSTICE INTELLIGENCE INFORMATION

### DISSEMINATION, ACCESS AND USE OF CRIMINAL JUSTICE INFORMATION—CRIMINAL JUSTICE AGENCIES

SEC. 201. (a) With limited exceptions hereafter described, direct access to criminal justice information should

be limited to authorized officers or employees of criminal justice agencies, established pursuant to Federal or State statute, and the use of such information should be limited to purposes of the administration of criminal justice.

(b) Consistent with regulations adopted by the Criminal Justice Information Systems Board, each criminal justice information system shall adopt procedures reasonably designed to insure—

(1) Conviction Record Information.—That routine exchanges between criminal justice agencies are limited to conviction record information;

(2) Arrest Record Information.—That exchanges of arrest record information or nonconviction record information between criminal justice agencies are carefully restricted to the following purposes—

(A) The screening of an employment application or review of employment by the criminal justice agency requesting the exchange with respect to its own employees or applicants,

(B) The commencement of prosecution, determination or pretrial or posttrial release or detention, the adjudication of criminal proceedings, or the preparation of a presentence report,

(C) The supervision by a criminal justice agency of an individual who had been committed

to the custody of that agency prior to the time on which the arrest occurred or the charge was filed,

(D) The investigation by a law enforcement agency of an individual when that individual has already been arrested or detained,

(E) The development of investigative leads by a law enforcement agency concerning an individual who has not been arrested, when the law enforcement agency requesting the information assures that there are specific and articulable facts which taken together with rational inferences from those facts warrant the conclusion that the individual has committed or is about to commit a criminal act and the information requested may be relevant to that act,

(F) The alerting of a law enforcement officer in the requesting agency that a particular individual may present a danger to his safety, or

(G) Similar essential purposes to which the information is relevant as defined in the procedures prescribed by the criminal justice agency;

(3) Correctional and Release Information.—That correctional and release information is disseminated only to criminal justice agencies or to the individual to whom the information pertains, or his attorney, where author-

ized by Federal or State statute, court rule, or court order.

DISSEMINATION OF IDENTIFICATION RECORD INFORMATION AND WANTED PERSONS RECORD INFORMATION

SEC. 202. Identification record information may be used or disseminated for any authorized purpose. Wanted person information may be used or disseminated for any authorized purpose relating to the administration of criminal justice.

DISSEMINATION, ACCESS AND USE OF CRIMINAL JUSTICE INFORMATION—NONCRIMINAL JUSTICE AGENCIES

SEC. 203. (a) Except as otherwise provided by this Act, conviction record information may be made available for purposes other than the administration of criminal justice only if expressly authorized by applicable Federal statute or State statute or if the information is to be made available to a Federal agency for such purpose if expressly authorized by Federal Executive order: *Provided, however,* That conviction record information may not be used for such purpose where prohibited by a State statute in the State where the conviction occurred.

(b) (1) Arrest record information indicating that an indictment, information, or formal charge has been made against an individual, has been made within twelve months of the date of the request for information, and is still pending, may be made available for a purpose other than the admin-

istration of criminal justice if the Criminal Justice Information Systems Board determines that access to that information is expressly and specifically authorized by a Federal statute or State statute or if the information is to be made available to a Federal agency for such purpose if expressly authorized by Federal Executive order: *Provided, however,* That conviction record information may not be used for such purpose where prohibited by a State statute in the State where the arrest occurred.

(2) Arrest record information furnished pursuant to this subsection may be used only for the purpose for which it was sought and may not be retained or copied by the requesting agency beyond the time necessary to accomplish the statutory purpose for which it was sought in the particular instance.

(c) When conviction record information or arrest record information is requested pursuant to this subsection, the requesting agency has the obligation to put the individual on notice that such information about him will be requested and that he has the right to seek review of this record for the purpose of challenge or correction.

(d) Criminal justice information may be made available to qualified persons for research related to the administration of criminal justice under regulations issued by the Criminal Justice Information Systems Board. Such regulations shall

require that the researcher preserve the anonymity of the individuals to whom such information relates, that nondisclosure agreements by all participants in the research program be completed, and that such additional requirements and conditions are met as the Board finds necessary to assure the protection of privacy and the security of the information. In formulating regulations pursuant to this section, the Board shall develop procedures designed to prevent this section from being used by criminal justice agencies to deny arbitrarily access to criminal justice information to qualified persons for research purposes where they have otherwise expressed a willingness to comply with regulations issued pursuant to this section.

(e) Where an organization is a criminal justice agency only by virtue of the fact that it has a contractual relationship with a Government agency to perform a function which is the administration of justice, or where a subunit of an agency is a criminal justice agency only by virture of the fact that it performs a function which is the administration of criminal justice, such organization or subunit shall be treated as a qualified person for research purposes pursuant to subsection (d) of this section. Such organization or subunit shall be required to complete nondisclosure agreements, shall comply with such requirements imposed upon it by this Act by virture of its being a criminal justice agency, and such addi-

tional requirements and conditions as the Board finds necessary to assure protection of privacy and the security of information.

(f) No provision of this Act shall prohibit an employee of a criminal justice agency from confirming to members of the news media or any other citizen that an individual is being detained, or incarcerated and the location of his detention or incarceration, or that an individual was arrested, detained, indicted, or that an information or other formal criminal charge was filed against the individual on a particular date at a particular place based on the employee's personal recollection or by reference to an original book of entry or police blotter maintained by a law enforcement agency at the place of original arrest or detention, not indexed or accessible by name and required to be made public, or by reference to court records of public criminal proceedings or official records of pardons or paroles indexed or accessible by date or indexed by name so long as such index only contains docket or file numbers of original court records. Where a court or criminal justice agency which maintains a record of pardons or paroles, also maintains a name index to original court, pardon on parole records containing criminal justice information in addition to docket or file numbers then unless prohibited by Federal or State statute the court or criminal justice agency must either maintain a separate name index

which contains only cross-references to the docket or file numbers to the original records, or it must provide upon request the docket number or numbers corresponding to any name in their index file.

(g) This Act applies to criminal justice information obtained from a foreign government or an international agency to the extent such information is contained in an information system subject to this Act. The Criminal Justice Information Systems Board shall take steps to assure that to the maximum extent feasible whenever any criminal justice information contained in information systems subject to this Act is provided to a foreign government or an international agency, that such information is used in a manner consistent with the provisions of this section.

DISSEMINATION, ACCESS, AND USE OF CRIMINAL JUSTICE INFORMATION—APPOINTMENTS AND EMPLOYMENT INVESTIGATIONS

SEC. 204. (a) A criminal justice agency may disseminate criminal justice information, whether or not sealed pursuant to section 208, criminal justice intelligence information, and criminal justice investigative information to a Federal, State, or local government official who is authorized by law to appoint or to nominate executive officers of law enforcement agencies, members of the Criminal Justice Information Systems Board, or any board or agency created or designated

pursuant to section 304, and to any legislative body authorized to approve such appointments. The criminal justice agency shall only disseminate such information concerning an individual upon notification from such official that he is considering that individual for such an office or from the legislative body that the individual has been nominated for the office and that the individual has been notified of the request for such information and has given his written consent to the release of the information.

(b) A criminal justice agency may disseminate arrest record information and criminal history information, whether or not sealed pursuant to section 208, to a Federal, State, or local government official who is not a criminal justice agency but who is authorized by law to appoint or nominate judges or executive officers of criminal justice agencies and to any legislative body authorized to approve such nominations. The criminal justice agency shall only disseminate such information concerning an individual upon notification from such official that he is considering that individual for such an office or from the legislative body that the individual has been nominated for the office and that the individual has been notified of the request for such information and has given his written consent to the release of the information.

(c) A criminal justice agency may disseminate arrest record information, criminal history record information,

whether or not sealed pursuant to section 208, to an agency of the Federal Government for the purpose of an employment application investigation, an employment retention investigation, or the approval of a security clearance for access to classified information, when the Federal agency requests such information as a part of a comprehensive investigation of the history and background of an individual, pursuant to an obligation to conduct such an investigation imposed by Federal statute or Federal Executive order, and pursuant to agency regulations setting forth the nature and scope of such an investigation. At the time he files his application, seeks a change of employment status, applies for a security clearance, or otherwise causes the initiation of the investigation, the individual shall be put on notice that such an investigation will be conducted and that access to this type of information will be sought.

(d) A criminal justice agency may disseminate criminal justice investigative information and criminal justice intelligence information to an agency of the Federal Government for the purpose of determining eligibility for security clearances allowing access to information classified as top secret when the Federal agency requests the criminal justice investigative or criminal justice intelligence information as a part of a comprehensive investigation of the history and background of an individual, pursuant to an obligation to conduct such an investigation imposed by Federal statute

or Federal Executive order, and pursuant to agency regulations setting forth the nature and scope of such an investigation. At the time he applies for a security clearance, the individual shall be put on notice that such an investigation will be conducted and that access to this type of information will be sought.

(c) Arrest record information, criminal history record information, criminal justice investigative information, and criminal justice intelligence information furnished pursuant to this section to an agency, official, or legislative body, may be used only for the purpose for which it is sought and may not be redisseminated, retained, or copied by the requestor beyond the time necessary to accomplish the statutory purpose for which it was sought in the particular instance.

SECONDARY USE OF CRIMINAL JUSTICE INFORMATION

SEC. 205. Any agency having access to, or receiving criminal justice information is prohibited, directly or through any intermediary, from disseminating such information to any individual or agency not authorized to have such information or from using such information for a purpose not authorized by this Act: *Provided, however,* That rehabilitation officials of criminal justice agencies with the consent of an individual under their supervision to whom the information refers may orally represent the substance of the individual's criminal history record information to prospective

employers or other individuals if such representation is, in the judgment of such officials and the individual or his attorney, if represented by counsel, helpful to obtaining employment or rehabilitation for the individual. In no event shall such correctional officials disseminate records or copies of records of criminal history record information to any unauthorized individual or agency. A court may disclose criminal justice information, criminal justice investigative information, or criminal justice intelligence information on an individual in a published opinion or in a public criminal proceeding.

METHOD OF ACCESS AND ACCESS WARRANTS FOR CRIMINAL JUSTICE INFORMATION

SEC. 206. (a) Except as provided in section 203 (d) or in subsection (b) of this section, an automated criminal justice information system may disseminate arrest record information, criminal history record information, or conviction record information on an individual only if the inquiry is based upon identification of the individual by means of name or other identification record information. The Criminal Justice Information Systems Board shall issue regulations to prevent dissemination of such information, except in the above situations, where inquiries are based upon categories of offense or data elements other than name and identification record information and to require that, after the arrest of an individual, such information concerning him shall

be available only on the basis of positive identification of him by means of fingerprints or other reliable identification record information.

(b) Notwithstanding the provisions of subsection (a) an automated criminal justice information system may disseminate arrest record information and conviction record information to law enforcement agencies where inquiries are based upon categories of offense or data elements other than identification record information if the information system has adopted procedures reasonably designed to insure that such information is used only for the purpose of developing investigative leads for a particular criminal offense and that the individuals to which such information is disseminated have a need to know and a right to know such information. Access to nonconviction record information contained in automated criminal justice information systems on the basis of data elements other than identification record information shall be permissible for the purpose of developing investigative leads for a particular criminal offense if the law enforcement agency seeking such access has first obtained a class access warrant from a United States Magistrate or a judge of competent jurisdiction. Such warrants may be issued as a matter of discretion by the judge in cases in which probable cause has been shown that (1) such access is imperative for purposes of the law enforcement agency's responsibilities in

the administration of criminal justice, and (2) the information sought to be obtained is not reasonably available from any other source or through any other method. A summary of each request for such a warrant, together with a statement of its disposition, shall within ninety days of disposition be furnished to the Criminal Justice Information Systems Board by the law enforcement agency.

SECURITY, ACCURACY, AND UPDATING OF CRIMINAL JUSTICE INFORMATION

SEC. 207. Consistent with regulations adopted by the Criminal Justice Information Systems Board, each criminal justice information system shall adopt procedures reasonably designed at a minimum—

(a) To insure the physical security of the system, to prevent the unauthorized disclosure of the information contained in the system, and to insure that the criminal justice information in the system is currently and accurately revised to include subsequently received information. The procedures shall also insure that all agencies to which such records are disseminated or from which they are collected are currently and accurately informed of any correction, deletion, or revision of the records. Such procedures adopted by automated systems shall provide that any other information system or agency which has direct access to criminal justice information contained in the automated system be informed as soon as feasi-



56-833 O - 75 - 6

ble of any disposition relating to arrest record information on an individual or any other change in criminal justice information in the automated system's possession.

(b) To insure that criminal justice agency personnel responsible for making or recording decisions relating to dispositions shall as soon as feasible report such dispositions to an appropriate agency or individual for entry into criminal justice information systems that contain arrest record information to which such dispositions relate.

(c) To insure that records are maintained with regard to—

(1) requests from any other agency or person for criminal justice information. Such records shall include the identity and authority of the requestor, the nature of the information provided, the nature, purpose, and disposition of the request, and pertinent dates;

(2) the source of arrest record information and criminal history information.

(d) To insure that information may not be submitted, modified, updated, or removed from any criminal justice information system without verification of the identity of the individual to whom the information refers and an indication of the person or agency submitting, modifying, updating, or removing the information.

(e) If the Criminal Justice Information Systems Board

finds that the additional cost of implementation of this section outweigh the interests of privacy which would be served by the implementation it may exempt the provisions of this section from application to information entered into a criminal justice information system prior to the effective date of this Act. The Criminal Justice Information Systems Board shall determine (by applying the same standard) the extent to which information entered into a criminal justice information system prior to the effective date of this Act should be exempted from other provisions of or requirements of this Act.

SEALING AND PURGING OF CRIMINAL JUSTICE INFORMATION

SEC. 208. (a) DISCRETIONARY SEALING OR PURGING—GENERALLY.—Consistent with regulations adopted by the Criminal Justice Information Systems Board, each criminal justice information system shall adopt procedures reasonably designed to insure that criminal justice information is purged or sealed when required by State or Federal statute, State or Federal regulations, or court order.

(b) MANDATORY SEALING.—Consistent with regulations adopted by the Criminal Justice Information Systems Board each criminal justice information system shall adopt procedures reasonably designed to insure that criminal justice information is sealed when, based on considerations of age, nature of the record, or the interval following the last entry

of information indicating that the individual is under the jurisdiction of a criminal justice agency, the information is unlikely to provide a reliable guide to the behavior of the individual. Procedures adopted pursuant to this subsection shall at a minimum provide—

(1) CONVICTION, NONCONVICTION, OR ARREST RECORDS.—For the prompt sealing or purging of criminal justice information relating to an individual who has been free from the jurisdiction or supervision of any criminal justice agency for—

(A) FELONY RECORDS.—A period of seven years, if the individual has previously been convicted of an offense for which imprisonment in excess of one year is permitted under the laws of the jurisdiction where the conviction occurred and such offense has not been specifically exempted from sealing by a Federal or State statute.

(B) NONFELONY RECORDS.—A period of five years, if the individual has previously been convicted of an offense for which the maximum penalty is not greater than imprisonment for one year under the laws of the jurisdiction where the conviction occurred, or

(C) NONCONVICTION OR ARREST RECORDS.—A period of two years following an arrest, deten-

tion, or formal charge, whichever comes first, if no conviction of the individual occurred during that period, no prosecution is pending at the end of the period, and the individual is not a fugitive; and

(2) NO PROSECUTION NONCONVICTION RECORDS.—For the prompt sealing of criminal history record information in any case in which a law enforcement agency has elected not to refer the case to the prosecutor or in which the prosecutor has elected not to file an information, seek an indictment or other formal criminal charge.

(3) PROMPTNESS OF SEALING.—That information eligible for sealing, contained in automated criminal justice information systems shall be sealed as soon as feasible. The Board may, in its discretion, permit a criminal justice information system which is not completely automated to determine the eligibility of information for sealing and to seal information at the time that access to that information is requested.

(4) INDEX OF SEALED RECORDS.—That an index of sealed records, consisting of identification record information on the individual whose record is sealed, is maintained in the jurisdiction where the arrest or detention occurred or where the individual was prosecuted or at a central repository of records. Information on such an index shall only be disseminated to a criminal justice

agency for the purpose of identifying an individual or determining whether a sealed record exists on an individual when the latter agency is able to point to specific and articulable facts which taken together with rational inferences from those facts warrant the conclusion that the individual has committed or is about to commit a criminal act and that the information may be relevant to that act. Within a criminal justice agency, access to and dissemination of information on such an index shall be on a need-to-know, right-to-know basis.

(5) ACCESS TO SEALED RECORDS.—That notwithstanding subparagraph (b) (1) or (b) (2) of this section, a record shall not be considered sealed—

(A) in connection with research pursuant to subsection 203 (d),

(B) in connection with a review pursuant to section 209 by the individual or his attorney,

(C) in connection with an audit conducted pursuant to section 306 or 311,

(D) where a record has been sealed pursuant to subparagraph (b) (1) (A) or (b) (1) (B) and the individual is subsequently arrested for an offense which is subject to imposition of a higher sentence under a Federal or State statute providing for additional penalties for repeat or habitual offenders,

(E) where the criminal justice agency seeking such access has obtained an access warrant from a State judge of competent jurisdiction if the information sought is in the possession of a State or local agency or information system, or from a Federal judge of competent jurisdiction, if the information sought is in the possession of a Federal agency or information system. Such warrants may be issued as a matter of discretion by the judge in cases in which probable cause has been shown that (1) such access is imperative for purposes of the criminal justice agency's responsibilities in the administration of criminal justice, and (2) the information sought to be obtained is not reasonably available from any other source or through any other method,

(F) where pursuant to section 204 an official, agency, or legislative body is permitted access to conviction record information for the purpose of screening an individual to be a judge, or an executive in a criminal justice agency or where an official or agency is permitted access to such information for the purpose of determining eligibility for a security clearance, or

(G) where an indictment, information, or other formal criminal charge is subsequently filed against the individual.

ACCESS BY INDIVIDUALS TO CRIMINAL JUSTICE INFORMATION FOR PURPOSES OF CHALLENGE

SEC. 209. (a) Any individual who believes that a criminal justice agency maintains arrest record information, criminal history information or wanted persons information concerning him, shall upon satisfactory verification of his identity, be entitled to review such information in person or through counsel in a method convenient to the individual; and to obtain a copy of it if needed for the purpose of challenge, correction, or the addition of explanatory material, or other specific purpose; and in accordance with rules adopted pursuant to this section, to challenge, purge, seal, delete, correct, and append explanatory material.

(b) Each criminal justice agency shall adopt and publish regulations to implement this section which shall, as a minimum, provide—

(1) the time, place, fees to the extent authorized by statute, and procedure to be followed by an individual or his counsel in gaining access to criminal justice information;

(2) that if on the basis of the review of such information, the individual believes such information to be inaccurate, incomplete, or maintained in violation of this Act, that he shall have a right to challenge such information in writing, and if there is no factual controversy

concerning the allegations in the individual's challenge, that the criminal justice agency maintaining the record shall expeditiously purge, seal, modify, or supplement the information. A failure to do so shall constitute a final action for the purpose of subsection 209(b)(7);

(3) that if there is a factual controversy concerning the allegations in the challenge, the agency shall request the agency responsible for original entry of the information to determine expeditiously the validity of the allegations; and that if the latter agency finds that there is a factual controversy, the agency shall upon written request of that individual convene a hearing on the challenge before an official of the agency authorized to purge, seal, modify, or supplement the information at which time the individual may appear with counsel, present evidence, and examine and cross-examine witnesses;

(4) any record found after such a hearing to be inaccurate, incomplete, or improperly maintained shall expeditiously be appropriately modified, supplemented, purged, or sealed;

(5) each criminal justice agency shall keep, and upon such a finding and upon request by the individual, disclose to such individual the name and authority of all persons, or organizations, to which and the date upon which such incomplete, inaccurate, or improperly main-

tained criminal justice information was disseminated during the period that the agency is required under section 207 (c) (1), and regulations implementing that section, to retain such records of dissemination;

(6) (A) the criminal justice agency to which the challenge is made shall give notice of the challenge each time it disseminates the challenged information and any agency or individual receiving such notice shall give similar notice each time it further disseminates the challenged information until such time as the challenge is finally resolved; and

(B) if any corrective action is taken as a result of a review or challenge filed pursuant to this section, the correcting agency shall give notice of such correction to each agency or individual to which it has disseminated the uncorrected information during the period that the agency is required to retain records of such disseminations, and shall instruct each such recipient to correct the information and to give similar notice to all agencies or individuals to which it has disseminated the uncorrected information during such record retention period; and

(7) the final action of a criminal justice agency on a request to review and challenge criminal justice information in its possession as provided by this section shall be reviewable pursuant to a civil action under section

309. The failure to act expeditiously as defined by regulations issued pursuant to section 303 shall be deemed a final action under this section.

(c) No individual who, in accord with this section, obtains information regarding himself may be required or requested to show or transfer records of that information to any other person or any other public or private agency or organization.

CRIMINAL JUSTICE INTELLIGENCE INFORMATION

SEC. 240. (a) Criminal justice intelligence information may be collected by a criminal justice agency only for official law enforcement purposes. It shall be maintained in a physically secure environment and shall not be entered in a criminal justice information system.

(b) Within the criminal justice agency maintaining the information, direct access to criminal justice intelligence information shall be limited to those officers or employees who have both a need to know and a right to know such information.

(c) Criminal justice intelligence information regarding an individual may be entered into a criminal justice intelligence information system only if grounds exist connecting such individual with known or suspected criminal activity and if the information is pertinent to such criminal activity. Criminal justice intelligence information shall be reviewed at reg-

ular intervals but at a minimum at the time such information is disseminated to determine whether such grounds exist, and if grounds do not exist such information shall likewise be purged.

(d) (1) Criminal justice intelligence investigative information may be disseminated from the criminal justice agency which collected such information only to a criminal justice agency or to a Federal agency authorized to receive the information pursuant to section 204 which has a need to know and a right to know such information and to individuals within the latter agency who have a need to know and a right to know such information.

(2) Criminal justice intelligence information on an individual may be disseminated from the criminal justice agency which collected such information only to a criminal justice agency—

(A) which needs the information to confirm the reliability of information supplied to the latter agency; or

(B) which is able to point to specific and articulable facts which taken together with rational inferences from those facts warrant the conclusion that the individual has committed or is about to commit a criminal act and that the information may be relevant to the act.

(e) When access to a criminal justice intelligence file is permitted under subsection (b) or information is dissemi-

nated pursuant to subsection (d) a record shall be kept of the identity of the person having access or the agency to which information was disseminated, the date of access or dissemination, and the purpose for which access was sought or information disseminated.

(f) Direct remote terminal access automated criminal justice intelligence information shall not be permitted outside the agency which collected and automated such information except where authorized by Federal statute or State statute: *Provided, however,* That remote terminal access shall be permitted to public record information maintained in intelligence files and to identification record information sufficient to provide an index of individuals included in the automated system and the names and locations of criminal justice agencies possessing additional information concerning such individuals and automatically referring the requesting agency's request to the agency maintaining more complete information.

(g) An assessment of criminal justice intelligence information may be provided to a governmental official or to any other individual when necessary to avoid imminent danger to life or property.

(h) The dissemination of criminal justice intelligence information to any government agency or employee of an agency by a criminal justice agency, or the use of such in-

formation by any government agency or employee of an agency, to influence a political campaign, discredit a candidate for office, or otherwise intimidate an individual in the exercise of rights guaranteed by the first amendment to the United States Constitution, shall constitute a violation of section 310.

(i) The Criminal Justice Information Systems Board shall conduct a study of the policies of criminal justice agencies concerning the collection of criminal justice intelligence information, and criminal justice investigative information, and the practices followed in the collection and dissemination of such information and shall issue guidelines setting forth the policies and practices necessary to insure protection of the privacy of individuals and the security of such information. It shall recommend to the Congress such additional measures as it deems necessary to insure the proper collection and use of criminal justice intelligence information and criminal justice investigative information.

(j) This Act applies to criminal justice intelligence obtained from a foreign government or an international agency to the extent such information is contained in an information system subject to this Act. The Criminal Justice Information Systems Board shall take steps to assure that to the maximum extent feasible whenever any criminal justice intelligence information contained in information systems subject

to this Act is provided to a foreign government or an international agency, that such information is used in a manner consistent with the provisions of this section.

CRIMINAL JUSTICE INVESTIGATIVE INFORMATION

SEC. 211. (a) Criminal justice investigative information may be disclosed pursuant to subsection 552 (b) (7) of title 5 of the United States Code or any similar State statute, or pursuant to any Federal or State statute, court rule, or court order permitting access to such information in the course of court proceedings to which such information relates.

(b) Except when such information is available pursuant to subsection (a), direct access to it shall be limited to those officers or employees of the criminal justice agency which maintains the information who have a need to know and a right to know such information and it shall be disseminated only to other governmental officers or employees who have a need to know and a right to know such information in connection with their civil or criminal law enforcement responsibilities. Records shall be kept of the identity of persons having access to files containing criminal justice investigative information or to whom such files are disseminated, the date of access or dissemination, and the purpose for which access is sought or files disseminated.

(c) Direct remote terminal access to automated criminal justice investigative files shall not be permitted outside the

agency which collected and automated such information except where authorized by Federal statute or State statute.

(d) Criminal justice investigative information shall not be entered in a criminal justice information system.

(e) Criminal justice investigative information may be made available to officers and employees of government agencies for the purposes set forth in section 204.

(f) The dissemination of criminal justice investigative information to any government agency or employee of an agency by a criminal justice agency, or the use of such information by any government agency or employee of an agency, to influence a political campaign, discredit a candidate for office, or otherwise intimidate an individual in the exercise of rights guaranteed by the first amendment to the United States Constitution, shall constitute a violation of section 310.

(g) This Act applies to criminal justice investigative information obtained from a foreign government or an international agency to the extent such information is contained in an information system subject to this Act. The Criminal Justice Information Systems Board shall take steps to assure that to the maximum extent feasible whenever any criminal justice investigative information contained in information systems subject to this Act is provided to a foreign government or an international agency, that such information is

used in a manner consistent with the provisions of this section.

## TITLE III—ADMINISTRATIVE PROVISIONS; REGULATIONS; CIVIL REMEDIES; CRIMINAL PENALTIES

### CRIMINAL JUSTICE INFORMATION SYSTEMS BOARD

SEC. 301. (a) CREATION AND MEMBERSHIP.—There is hereby created a Criminal Justice Information Systems Board (hereinafter the "Board") which shall have overall responsibility for the administration and enforcement of this Act. The Board shall be composed of thirteen members. One of the members shall be the Attorney General and two of the members shall be designated by the President as representatives of other Federal agencies outside of the Department of Justice. One of the members shall be designated by the Judicial Conference of the United States. The nine remaining members shall be appointed by the President with the advice and consent of the Senate. Of the nine members appointed by the President, seven shall be officials of criminal justice agencies from seven different States at the time of their nomination, representing to the extent possible all segments of the criminal justice system. The two remaining Presidential appointees shall be private citizens well versed in the law of privacy, constitutional law, and information systems technology. The President shall designate one of the seven criminal

56-833 O - 75 - 7

justice agency officials as Chairman and such designation shall also be confirmed by the advice and consent of the Senate. Not more than seven members of the Board shall be of the same political party.

(b) TERMS OF OFFICE AND VACANCIES.—The two members of the Board designated by the President as representatives of other Federal agencies outside of the Department of Justice shall serve at the pleasure of the President. The member designated by the United States Judicial Conference shall serve at the pleasure of the Conference. Four of the Presidential appointees first appointed pursuant to this Act shall continue in office for terms of six years. The remaining Presidential appointees first appointed pursuant to this Act shall continue in office for the terms of one, two, three, four, and five years, respectively, from the date of the effective date of this Act, the term of each to be designated by the President: *Provided, however,* That their successors shall be appointed for terms of six years and until their successors are appointed and have qualified, except that they shall not continue to serve beyond the expiration of the next session of Congress subsequent to the expiration of said fixed term of office. Any person chosen to fill a vacancy shall be appointed only for the unexpired term of the Board member whom he succeeds. No vacancy in the Board shall impair the right of the remaining members to exercise all the powers of the

Board. Seven members shall constitute a quorum for the transaction of business.

(c) COMPENSATION OF MEMBERS.—

(1) Each member of the Board who is not otherwise in the service of the Government of the United States shall receive a sum equivalent to the compensation paid at level IV of the Federal Executive Salary Schedule, pursuant to section 5315 of title 5, prorated on a daily basis for each day spent in the work of the Board, and shall be paid actual travel expenses, and per diem in lieu of subsistence expenses when away from his usual place of residence, in accordance with section 5 of the Administrative Expenses Act of 1946, as amended.

(2) Each member of the Board who is otherwise in the service of the Government of the United States shall serve without compensation in addition to that received for such other service, but while engaged in the work of the Board shall be paid actual travel expenses, and per diem in lieu of subsistence expenses when away from his usual place of residence, in accordance with the provisions of the Travel Expenses Act of 1949, as amended.

(3) Members of the Board shall be considered

"special Government employees" within the meaning of section 202 (a) of title 18.

(d) AUTHORITY.—For the purpose of carrying out its responsibilities under the Act, the Board shall have authority,

(1) after notice and hearings to issue regulations as required by section 303;

(2) to issue an order prohibiting the exchange of criminal justice information (except wanted persons information), criminal justice investigative information, or criminial justice intelligence information with a criminal justice agency which has not satisfied the requirements of section 304;

(3) to exercise the powers set out in section 308;

(4) to bring actions under section 309 for declaratory and injunctive relief;

(5) to supervise the operation of an automated information system for the exchange of criminal justice information among the States and with the Federal Government pursuant to section 307;

(6) to supervise the installation and operation of any criminal justice information system, criminal justice investigative information system or criminal justice intelligence information system operated by the Federal Government;

(7) to issue an order prohibiting the establishment

of any new information system covered by this Act and operated by the Federal Government or prohibiting the expansion of any such existing system where the Board finds such establishment or expansion to be either inconsistent with this Act or without adequate statutory authority;

(8) to conduct an ongoing study of the policies of various agencies of the Federal Government in the operation of information systems;

(9) to require any department or agency of the Federal Government or any criminal justice agency to submit to the Board such information and reports with respect to its policy and operation of information systems or with respect to its collection and dissemination of criminal justice information, criminal justice investigative information, or criminal justice intelligence information and such department or agency shall submit to the Board such information and reports as the Board may reasonably require;

(10) to conduct audits as required by section 306; and

(11) to create such advisory committees as it deems necessary.

(e) OFFICERS AND EMPLOYEES.—There shall be a full-time staff director for the Board who shall be appointed by

the Board and who shall receive compensation at the rate provided for level V of the Federal Executive Salary Schedule, pursuant to section 5316 of title 5. Within the limitation of appropriations, the Board may appoint such other personnel as it deems advisable, in accordance with the civil service and classification laws, and may procure services as authorized by section 3109 of title 5, but at rates for individuals not in excess of the daily equivalent paid for positions at the maximum rate for GS–15 of the General Schedule under section 5332 of title 5.

(f) REPORT TO CONGRESS AND TO THE PRESIDENT.—The Board shall issue an annual report to the Congress and to the President. Such report shall at a minimum contain—

(1) the results of audits conducted pursuant to section 306;

(2) a summary of orders issued pursuant to subsections (d) (2), (d) (3), and (d) (7) and actions brought pursuant to subsection (d) (4) of this section;

(3) a summary of public notices filed by criminal justice information systems, criminal justice investigative information systems, criminal justice intelligence information systems, and criminal justice agencies pursuant to section 305; and

(4) any recommendations the Board might have for new legislation on the operation or control of in-

formation systems or on the collection and control of criminal justice information, criminal justice investigative information, or criminal justice intelligence information.

HEARINGS AND WITNESSES

SEC. 302. (a) The Board, or on authorization of the Board, any subcommittee or three or more members may hold such hearings and act at such times and places as necessary to carry out the provisions of this Act. Hearings shall be public except to the extent that the hearings or portions thereof are closed by the Board in order to protect the privacy of individuals or the security of information protected by this Act.

(b) Each member of the Board shall have the power and authority to administer oaths or take statements from witnesses under affirmation.

(c) A witness attending any session of the Board shall be paid the same fees and mileage paid witnesses in the courts of the United States. Mileage payments shall be tendered to the witness upon service of a subpena issued on behalf of the Commission or any subcommittee thereof.

(d) Subpenas for the attendance and testimony of witnesses or the production of written or other matter, required by the Board for the performance of its duties under this Act, may be issued in accordance with rules or procedure

established by the Board and may be served by any person designated by the Board.

(e) In case of contumacy or refusal to obey a subpena any district court of the United States or the United States court of any territory or possession, within the jurisdiction of which the person subpenaed resides or is domiciled or transacts business, or has appointed an agent for the receipt of service of process, upon application of the Board, shall have jurisdiction to issue to such person an order requiring such person to appear before the Board or a subcommittee thereof, there to produce pertinent, relevant, and nonprivileged evidence if so ordered, or there to give testimony touching the matter under investigation; and any failure to obey such order of the court may be punished as contempt.

(f) Nothing in this Act prohibits a criminal justice agency from furnishing the Board information required by it in the performance of its duties under this Act.

FEDERAL REGULATIONS

SEC. 303. (a) Except as provided in subsection (b) of this section, the Board shall, after consultation with representatives of State and local criminal justice agencies participating in information systems covered by this Act and other interested parties, and after notice and hearings, promulgate such interpretations, rules, regulations, and procedures as it may deem necessary to effectuate the provisions of

this Act. The Board shall follow the provisions of the Administrative Procedures Act with respect to the issuance of such rules. At least sixty days prior to their promulgation, the Board shall refer any interpretations, rules, regulations, or procedures which will affect the collection and dissemination of information maintained by State or local criminal justice agencies to the Governor of each State, any agency created or designated pursuant to section 304, any other organizations or individuals in a State designated by the Governor and any other organizations or individuals requesting to be so notified. At least sixty days prior to their promulgation, the Board shall also refer any interpretations, rules, regulations, or procedure which will affect the collection and dissemination of information maintained by Federal criminal justice agencies to the Department of Justice, each such Federal criminal justice agency and the United States Judicial Conference for their review. The Board may in its discretion refer any interpretations, regulations, or procedures prior to promulgation to any other advisory committee it may create. All regulations issued by the Board or any criminal justice agency pursuant to this Act shall be published and easily accessible to the public.

(b) The Board shall not have authority to issue regulations involving criminal justice information on an arrest or indictment for a Federal offense; or criminal justice intelli-

gence information or criminal justice investigative information resulting from the investigative activities of a Federal criminal justice agency: *Provided, however,* That the Board shall have authority to issue regulations involving criminal justice information on an arrest or indictment for a Federal offense if such information is maintained in an information system operated pursuant to section 307. Regulations concerning information exempted from the Board's jurisdiction pursuant to this subsection shall be issued by Executive order of the President upon recommendation of the Attorney General, the two members of the Board designated by the President and the member designated by the Judicial Conference of the United States.

STATE REGULATIONS AND CREATION OF STATE INFORMATION SYSTEMS BOARDS

SEC. 304. No criminal justice agency shall disseminate criminal justice information (except wanted persons information), criminal justice intelligence information, or criminal justice investigative information to a criminal justice agency—

(a) which has not adopted all of the operating procedures required by title II of the Act; or

(b) which is located in another State which has failed to either create an agency or designate an existing

agency which has statewide authority and responsibility for:

(1) the enforcement of the provisions of this Act and any State statute which serves the same goals;

(2) the issuance of regulations, not inconsistent with this Act, regulating the exchange of criminal justice information, criminal justice investigative information, and criminal justice intelligence information and the operation of criminal justice information systems, criminal justice intelligence information systems, and criminal justice investigative information systems; and

(3) the supervision of the installation of criminal justice information systems, criminal justice investigative information systems and criminal justice intelligence information systems, the exchange of information by such systems within that State and with similar systems and criminal justice agencies in other States and in the Federal Government.

PUBLIC NOTICE REQUIREMENT

SEC. 305. (a) Any criminal justice agency maintaining an automated criminal justice information system, an automated criminal justice investigative information system, or an

automated criminal justice intelligence information system; any Federal criminal justice agency maintaining any such information system, whether or not automated, and any criminal justice agency maintaining a statewide or regional criminal justice information system, whether or not automated, or any such agency maintaining a criminal justice information system containing criminal justice information on more than 10,000 individuals shall give public notice of the existence and character of its system once each year. Any such agency maintaining more than one system shall publish such annual notices for all its systems simultaneously. Any such agency proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall be transmitted to the Board and shall specify—

(1) the name of the system;

(2) the nature and purposes of the system;

(3) the categories and number of persons on whom data are maintained;

(4) the categories of data maintained, indicating which categories are stored in computer-accessible files;

(5) the agency's operating rules and regulations issued pursuant to title II of the Act, the agency's poli-

cies and practices regarding data information storage, duration of retention of information, and disposal thereof;

(6) the categories of information sources;

(7) a description of all types of use made of information, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them;

(8) the title, name, and address of the person immediately responsible for the operation of the system; and

(9) in the case of any agency proposing to establish a new system or to enlarge an existing system, a privacy impact statement describing the consequences to the individual, including his rights, privileges, benefits, detriments, and burdens, of the proposed new system or the proposed expansion of an existing system.

(b) Any criminal justice agency, criminal justice information system, criminal justice investigative information system, or criminal justice intelligence information system operated by the Federal Government shall satisfy the public notice requirement set out in subsection (a) of this section by publishing the information required by that subsection in the Federal Register.

ANNUAL AUDIT

SEC. 306. (a) At least once annually the Board shall conduct a random audit of the practices and procedures of the Federal agencies which collect and disseminate information pursuant to this Act to insure compliance with its requirements and restrictions. The Board shall also conduct such an audit of at least ten statewide criminal justice information systems each year and of every statewide and multistate system at least once every five years. The Board may at any time conduct such an audit of any criminal justice agency or information system covered by this Act when the Board has reason to believe the agency or information system is maintaining, disseminating, or using information in violation of this Act.

(b) Each criminal justice information system shall conduct a similar audit of its own practices and procedures once annually. Each State agency created pursuant to subsection 304(b) shall conduct an audit on each criminal justice information system, each criminal justice investigative information system, and each criminal justice intelligence information system operating in that State on a random basis, at least once very five years.

(c) The results of such audits shall be made available to the Board which shall report the results of such audits once annually to the Congress by May 1 of each year begin-

ning on May 1 following the expiration of the first twelve-calendar-month period after the effective date of the Act.

(d) Notwithstanding any provision contained in title II of this Act, members and staff of the Board or any State agency designated or created pursuant to section 304 shall have access to such information covered by this Act as is necessary to conduct audits pursuant to this section.

A NATIONAL CRIMINAL JUSTICE INFORMATION SYSTEM

SEC. 307. (a) Subject to the limitations of subsections (b) and (c) of this section, the Board may authorize a Federal criminal justice agency or federally chartered corporation to operate an interstate criminal justice information system, either manual or automated or both. The Board shall have authority to determine the extent to which the Federal criminal justice agency or Federal corporation may maintain its own telecommunications system.

(b) Any information system operated by the agency or Federal corporation may include criminal history record information on an individual relating to a violation of the criminal laws of the United States, a violation of the laws of another nation or violations of the laws of two or more States. As to all other individuals criminal justice information included in the agency's information system shall consist only of information sufficient to establish the identity of the individuals, and the identities and locations of criminal justice

agencies possessing other types of criminal justice information concerning such individuals.

(c) Notwithstanding the provisions of subsection (b), the agency or Federal corporation may maintain criminal history record information submitted by a State which otherwise would be unable to participate fully in an interstate criminal history record information system because of the lack of facilities or procedures but only until such time as such State is able to provide the facilities and procedures to maintain the records in the State, and in no case beyond the fifth twelve-calendar-month period after the date of enactment. Criminal history record information maintained in Federal facilities pursuant to this subsection shall be limited to information on offenses for which imprisonment in excess of one year is permitted under the laws of the jurisdiction where the offense occurred.

ADMINISTRATIVE PENALTIES

SEC. 308. If the Board finds that any criminal justice agency has violated any provision of this Act, after notice and hearings it may (1) issue orders or bring actions as authorized by section 301, (2) interrupt or terminate the exchange of information authorized to be exchanged by this Act, or (3) interrupt or terminate the use of Federal funds for the operation of such a system or agency, or (4) require the system or agency to return Federal funds dis-

tributed in the past, or (5) require the system or agency to discipline any employee responsible for such violation or (6) take any combination of such actions.

CIVIL REMEDIES

SEC. 309. (a) Any person aggrieved by a violation of this Act or regulations promulgated thereunder shall have a civil action for damages or any other appropriate remedy against any person, system, or agency responsible for such violation. An action alleging a violation of section 209 shall be available only after he has exhausted the administrative remedies provided by that section.

(b) The Board shall have a civil action for declaratory judgments, cease-and-desist orders, and such other injunctive relief as may be appropriate against any criminal justice agency, criminal justice information system, criminal justice intelligence information system, or criminal justice investigative information system.

(c) If a defendant in an action brought under this section is an officer or employee or agency of the United States the action shall be brought in an appropriate United States district court. If the defendant or defendants in an action brought under this section are private persons or officers or employees or agencies of a State or local government, the action may be brought in an appropriate United States district court or in any other court of competent jurisdiction.

56-833 O - 75 - 8

The district courts of the United States shall have jurisdiction over actions described in this section without regard to the amount in controversy.

(d) In any action brought pursuant to this Act, the court may in its discretion issue an order enjoining maintenance or dissemination of information in violation of this Act, or correcting records of such information or any other appropriate remedy except that in an action brought pursuant to subsection (b) the court may order only declaratory or injunctive relief.

(e) In an action brought pursuant to subsection (a), any person aggrieved by a violation of this Act shall be entitled to actual and general damages but not less than liquidated damages of a $100 recovery for each violation and reasonable attorneys' fees and other litigation costs reasonably incurred. Exemplary and punitive damages may be granted by the court in appropriate cases brought pursuant to subsection (a). Any person, system, or agency responsible for violations of this Act shall be jointly and severally liable to the person aggrieved for damages granted pursuant to this subsection: *Provided, however,* That good faith reliance by an agency or information system, or employee of such agency or system upon the assurance of another agency, information system, or employee that information provided the former agency, information system, or

employee is maintained or disseminated in compliance with the provisions of this Act or any regulations issued thereunder shall constitute a complete defense for the former agency, system, or employee to a civil damage action brought under this section but shall not constitute a defense with respect to equitable relief.

(f) For the purposes of this Act the United States shall be deemed to have consented to suit and any agency or system operated by the United States found responsible for a violation shall be liable for damages, reasonable attorney's fees, and litigation costs as provided in subsection (e) notwithstanding any provisions of the Federal Tort Claims Act.

(g) A determination by a court of a violation of internal operating procedures adopted pursuant to this Act should not be a basis for excluding evidence in a criminal case unless the violation is of constitutional dimension or is otherwise so serious as to call for the exercise of the supervisory authority of the court.

CRIMINAL PENALTIES

SEC. 310. Any government employee who willfully disseminates, maintains, or uses information knowing such dissemination, maintenance, or use to be in violation of this Act shall be fined not more than $5,000 or imprisoned for not more than five years, or both.

AUDIT AND ACCESS TO RECORDS BY THE GENERAL ACCOUNTING OFFICE

SEC. 311. (a) The Comptroller General of the United States shall from time to time, at his own initiative or at the request of either House or any committee of the House of Representatives or the Senate or any joint committee of the two Houses, conduct audits and reviews of the activities of the Board under this Act. For such purposes, the Comptroller General, or any of his duly authorized representatives, shall have access to and the right to examine all books, accounts, records, reports, files, and all other papers, things, and property of—

(1) the Board,

(2) any Federal agencies audited by the Board pursuant to section 306(a) of this Act, and

(3) any statewide and multistate information systems, including organizations and agencies thereof, audited by the Board pursuant to section 306(a) of this Act,

which, in the opinion of the Comptroller General, may be related or pertinent to his audits and reviews of the activities of the Board. In the case of agencies and systems referred to in paragraphs (2) and (3), the Comptroller General's right of access shall apply during the period of audit by the Board and for three years thereafter.

(b) Notwithstanding any other provision of this Act, the Comptroller General's right of access to books, accounts, records, reports, and files pursuant to and for the purposes specified in subsection (a) shall include any information covered by this Act. However, no official or employee of the General Accounting Office shall disclose to any person or source outside of the General Accounting Office any such information in a manner or form which identifies directly or indirectly any individual who is the subject of such information.

PRECEDENCE OF STATE LAWS

SEC. 312. (a) Any State law or regulation which places greater restrictions upon the dissemination of criminal justice information, criminal justice intelligence information, criminal justice investigative information or the operation of criminal justice information systems, criminal justice intelligence information systems, criminal justice investigative information systems or which affords to any individuals, whether juveniles or adults, rights of privacy or protections greater than those set forth in this Act shall take precedence over this Act or regulations issued pursuant to this Act.

(b) Except with respect to information maintained by an information system created pursuant to section 307, any State law or regulation which places greater restrictions upon the dissemination of criminal justice information, criminal

justice intelligence information or criminal justice investigative information or the operation of criminal justice information systems, criminal justice intelligence information systems or criminal justice investigative information systems or which affords to any individuals, whether juveniles or adults, rights of privacy or protections greater than those set forth in the State law or regulations of another State shall take precedence over the law or regulations of the latter State where such information is disseminated from an agency or information system in the former State to an agency, information system, or individual in the latter State. Subject to court review pursuant to section 309, the Board shall be the final authority to determine whether a State statute or regulation shall take precedence under this section and shall as a general matter have final authority to determine whether any regulations issued by a State agency, a criminal justice agency, or information system violate this Act and are therefore null and void.

(c) The Board may in its discretion suspend the application of this section for criminal justice information maintained by a Federal corporation or Federal criminal justice agency pursuant to section 307 (c). The Board may not suspend the application of this section beyond the date of expiration of the fifth twelve-calendar-month period following the date of enactment of this Act.

APPROPRIATIONS AUTHORIZED

SEC. 313. For the purpose of carrying out the provisions of this Act, there are authorized to be appropriated such means as the Congress deems necessary.

SEVERABILITY

SEC. 314. If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of the Act and the application of the provision to other persons not similarly situated or to other circumstances shall not be affected thereby.

REPEALERS

SEC. 315. The second paragraph under the headings entitled "Federal Bureau of Investigation; Salaries and Expenses" contained in the "Department of Justice Appropriations Act, 1973" is hereby repealed.

EFFECTIVE DATE

SEC. 316. The provisions of this Act shall take effect upon the date of expiration of the second twelve-calendar-month period following the date of the enactment of this Act: *Provided, however,* That section 313 of this Act shall take effect upon the date of enactment of this Act and that members, officers, and employees of the Board may be appointed and take office at any time after the date of enactment. The Board may delay the effective date of any provision of this Act: *Provided, however,* That the effective date of no provi-

64

sion of this Act shall be delayed beyond the third twelve-calendar-month period following the date of enactment of this Act.

94TH CONGRESS
1ST SESSION

# S. 1428

IN THE SENATE OF THE UNITED STATES

APRIL 14, 1975

MR. TUNNEY introduced the following bill; which was read twice and referred to the Committee on the Judiciary

# A BILL

To provide for the security, accuracy, and confidentiality of criminal justice information and to protect the privacy of individuals to whom such information relates, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,* That this Act may be cited as the "Criminal Justice Information Control and Protection of Privacy Act of 1975".

## TITLE I—PURPOSE AND SCOPE

### FINDINGS

SEC. 101. The Congress hereby finds and declares that—

(a) The responsible exchange of complete and accurate criminal justice information among criminla justice agencies

is recognized as necessary and indispensable to effective law enforcement and criminal justice and is encouraged.

(b) Individual rights, however, may be infringed if information is inaccurate, incomplete, or is disseminated irresponsibly.

(c) While the enforcement of criminal laws and the regulation of criminal justice information systems is primarily the responsibility of State and local government, the Federal Government has a substantial and interconnected role.

(d) This Act is based on the powers of the Congress—

(1) to place reasonable restrictions on Federal activities and upon State and local governments which received Federal grants or other Federal services or benefits, and

(2) to facilitate and regulate interstate commerce.

DEFINITIONS

SEC. 102. As used in this Act—

(1) "Arrest record information" means notations of the arrest, detention, or indictment, or filing of an information, or other formal criminal charge, against an individual, made by a criminal justice agency, which do not include a disposition.

(2) "Automated" means utilizing electronic computers or other automatic data processing equipment, as distinguished from performing operations manually.

(3) "Correctional and release information" means information on an individual compiled by an agency in connection with bail, pretrial or posttrial release proceedings, reports on the physical or mental condition of an alleged offender, reports on presentence investigations, reports on inmates in correctional institutions or participants in rehabilitation programs, and probation and parole reports.

(4) "Criminal record information" means information compiled by a criminal justice agency on an individual consisting of notations of arrest, detention, indictment, information, or other formal criminal charge together with a disposition thereof.

(5) "Criminal justice" refers to the activities of a criminal justice agency relating to protection against, detection of, or investigation of criminal offenses, or to the apprehension, detention, pretrial release, posttrial release, prosecution, defense, correctional supervision or rehabilitation of accused persons or criminal offenders, adjudication of a charge, or processing requests for executive clemency.

(6) "Criminal justice agency" means a court or any other governmental agency or subunit thereof which as its principal function performs criminal justice activities and any other agency or subunit thereof which performs criminal justice activities but only to the extent that it does so.

(7) "Criminal justice information" includes arrest

record information, criminal record information, correctional and release information, criminal justice intelligence information and criminal justice investigative information.

(8) "Criminal justice intelligence information" means information collected by a criminal justice agency with respect to an identifiable individual or groups of individuals in an effort to anticipate, prevent, or monitor possible criminal activity.

(9) "Criminal justice investigative information" means information with respect to an indentifiable individual compiled by a criminal justice agency in the course of conducting a criminal investigation of a specific act or omission, including information derived from reports of investigators or informants, or from any type of surveillance.

(10) "Disposition" means that (A) criminal proceedings have been concluded; (B) a law enforcement agency has elected not to refer a matter for prosecution; (C) a prosecutor has elected not to commence criminal proceedings; or (D) criminal proceedings have been indefinitely postponed. "Disposition" includes but is not limited to, acquittal, acquittal by reason of insanity or mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity or mental incompetence, charge still pending due to insanity or mental incompetence, guilty plea,

nolle prosequi, no paper, nolo contendere plea, convicted, deceased, deferred disposition, dismissed-civil action, extradited, found insane or incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial-defendant discharged.

(11) "Executive order" means an order of the President of the United States or the chief executive of a State which has the force of law and which is published in a manner permitting regular public access thereto.

(12) "Law enforcement agency" means a criminal justice agency which is empowered by law to make arrests.

(13) "State" includes any of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

APPLICABILITY

SEC. 103. (a) This Act applies to any criminal justice agency—

(1) of the Federal Government,

(2) of a State or local government which is funded in whole or in part by the Federal Government,

(3) which exchanges information interstate, and

(4) which exchanges information with an agency covered by paragraph (1), (2), or (3) but only to the extent of that exchange.

(b) The provisions of this Act do not apply to—

(1) original records of entry such as police blotters maintained by criminal justice agencies, indexed chronologically and permitted by law to be made public, if such records are organized on a chronological basis,

(2) court records of public criminal proceedings,

(3) public criminal proceedings and court opinions, including published compilations thereof,

(4) records of traffic offenses disseminated to or maintained by departments of transportation, motor vehicles, or the equivalent, primarily for the purpose of regulating the issuance, suspension, revocation, or renewal of drivers' or other operators' licenses,

(5) records relating to violations of the Uniform Code of Military Justice but only so long as those records are maintained solely within the Department of Defense,

(6) statistical or analytical records or reports in which individuals are not identified and from which their identities are not ascertainable,

(7) announcements of executive elemency, or

(8) criminal justice intelligence information or criminal justice investigative information specifically required by Federal Executive order to be kept secret in the interest of national defense or foreign policy.

## TITLE II—COLLECTION, DISSEMINATION, AND USE OF CRIMINAL JUSTICE INFORMATION

### USE OF INFORMATION BY CRIMINAL JUSTICE AGENCIES

SEC. 201. (a) Criminal justice information shall be exchanged, disseminated, and used only in the manner provided by this Act. Criminal justice agencies may exchange criminal justice information among themselves for criminal justice purposes, consistent with the provisions of this Act. To secure these objectives, each criminal justice agency, after notice and an opportunity for public comment, shall promulgate and publish regulations which—

(1) specify the type of criminal justice information systems maintained,

(2) require compliance with the provisions of this Act and regulations and procedures established pursuant thereto,

(3) specify limits on dissemination, exchange, and use of criminal justice information, and

(4) provide appropriate sanctions for noncompliance with the provisions of this Act and regulations and procedures adopted pursuant thereto.

(b) Each criminal justice agency shall adopt internal operating procedures reasonably designed to—

(1) prevent unauthorized access to, or dissemination of, criminal justice information; and

(2) insure that correctional and release information is disseminated only to (A) criminal justice agencies, (B) the individual to whom the information pertains, or his attorney, when authorized by Federal or State statute, court rule or court order, or (C) individuals authorized to receive it under sections 205 and 206.

(c) A law enforcement agency shall adopt procedures reasonably designed to insure that arrest record information which is accessed for the purpose of developing investigative leads concerning an individual who has not yet been arrested, does not, without additional information, provide the basis for a subsequent detention or arrest. If the arrest record information is obtained from another criminal justice agency, a record is required as to the identity of the requesting officer, the information obtained, the purpose of the request for information, and the use of the information. These records shall be maintained for a minimum of three years and shall be reviewed by the requesting agency periodically to insure compliance with this subsection.

(d) Information contained in a criminal justice information system which was obtained from a foreign government or international organization is subject to the same restrictions and limitations on use as information in the system obtained from domestic sources. Criminal justice infor-

mation may be exchanged with foreign governments or international organizations pursuant to treaties or formal or informal agreements. Whenever such information is exchanged with a foreign government or international organization, such government or organization should be encouraged to use it in a manner consistent with the purposes of this Act.

IDENTIFICATION AND WANTED PERSON INFORMATION

SEC. 202. Identification information including fingerprints and photographs may be used or disseminated for any official purpose but identification information which includes arrest record information or criminal record information may be disseminated only as permitted by this Act. Information that a person is wanted for a criminal offense and that judicial process has been issued against him, together with an appropriate description and other information which may be of assistance in locating the person or demonstrating a potential for violence. Nothing in this Act prohibits direct access by a criminal justice agency to automated wanted person or stolen property information.

ACCESS TO AUTOMATED CRIMINAL JUSTICE INFORMATION SYSTEMS

SEC. 203. (a) Exchanges of criminal justice information between criminal justice agencies by means of automated systems shall be governed by formal written agreements

specifying the duration of the agreement, the type of information to be exchanged, the persons having direct access to the information, the security provisions necessary to protect the information, and such other matters as are necessary to insure compliance with law.

(b) A criminal justice agency shall adopt procedures reasonably designed to insure that—

(1) whenever feasible, arrest record information or criminal record information in an automated system is accessed on the basis of a specific identification number or other accurate identifier,

(2) whenever arrest record information or criminal record information is accessed by patrol units by means of automated systems, records are required as to the identity of the requesting officer, the information obtained, the purpose of the request, and the use of the information, and these records shall be maintained for a minimum of three years.

DISSEMINATION, ACCESS, AND USE—NONCRIMINAL JUSTICE AGENCIES

SEC. 204. (a) Criminal record information may be made available for noncriminal justice purposes only as provided in this Act or where authorized by applicable Federal or State statute or Executive order.

(b) When requested, arrest record information indicat-

ing that an indictment, information, or formal charge against an individual has been filed within twelve months of the date of the request therefor, or is still pending, may be made available for a noncriminal justice purpose where authorized by Federal or State statute or Executive order. Other arrest record information may be made available for a noncriminal justice purpose only as provided in subsections (d) and (e) of this section and subsections (a) and (b) of section 205, or when expressly provided in a Federal or State statute. Arrest record information made available as permitted by this subsection may be used only for the purpose for which it was requested, and may not be retained by the requestor beyond the time necessary to accomplish the purpose for which it was sought.

(c) A requestor who is entitled to obtain arrest record information or criminal record information as permitted by subsection (a) or (b), has the obligation to put individuals who may be the subject of such records on notice that such information may be requested.

(d) A criminal justice agency may disseminate criminal justice information, upon request, to officers and employees of the Immigration and Naturalization Service, consular officers, and officers and employees of the Visa Office of the Department of State, who require such information for the purpose of administering the immigration

and nationality laws. The Attorney General and the Secretary of State shall adopt internal operating procedures reasonably designed to insure that arrest record information received pursuant to this subsection is used solely for the purpose of developing further investigative leads and that no decision adverse to an individual is based on arrest record information unless there has been a review of the decision at a supervisory level.

(e) A criminal justice agency may disseminate criminal justice information, upon request, to officers and employees of the Bureau of Alcohol, Tobacco and Firearms, the United States Customs Service and Internal Revenue Service and the Office of Foreign Assets Control of the Department of the Treasury, who require such information for the purpose of administering those laws under their respective jurisdictions. The Secretary of the Treasury shall adopt internal operating procedures reasonably designed to insure that arrest record information received pursuant to this subsection is used solely for the purpose of developing further investigative leads and that no decision adverse to an individual is based on arrest record information unless there has been a review of the decision at a supervisory level.

(f) The Drug Enforcement Administration of the United States Department of Justice may disseminate crimi-

nal record information to federally registered manufacturers and distributors of controlled substances.

(g) A criminal justice agency shall adopt procedures relating to access to arrest record information, criminal record information, and correctional and release information by individuals and agencies for research, evaluative, or statistical activities. Where research is authorized, such procedures shall include the requirement of a formal agreement between the individual or agency performing the research and the criminal justice agency specifically authorizing access to data, limiting the use of the data to research, evaluative, or statistical purposes, insuring the confidentiality and security of the data consistent with this Act, and providing sanctions for the violations of this Act or the terms of the agreement.

(h) A nongovernmental organization which performs criminal justice functions within the meaning of this Act is required to undertake a formal agreement with a criminal justice agency. The agreement shall (1) provide that access to criminal justice information is obtained through the criminal justice agency with which the agreement is made; (2) indicate specifically the type of data to which access is permitted; (3) limit the use of the data to the purpose for which it is sought; (4) insure the confidentiality and secu-

rity of data; (5) provide for recordkeeping and review consistent with the provisions of section 207(a) (4) and (6), respectively; and (6) provide for termination of the agreement for failure to comply with these requirements.

(i) Nothing in this Act prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates. Nor is a criminal justice agency prohibited from confirming prior arrest record information or criminal record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charges was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by section 103(b) from the application of this Act.

ACCESS FOR APPOINTMENTS AND EMPLOYMENT INVESTIGATIONS

SEC. 205. (a) A criminal justice agency may disseminate criminal justice information—

(1) for the purpose of screening employment ap-

plications or reviewing employment for a criminal justice agency,

(2) to a Federal, State, or local government official who is authorized by law to appoint or nominate judges or executive officers of criminal justice agencies or members of the Commission on Criminal Justice Information, and

(3) to any legislative body authorized to approve appointments made pursuant to paragraph (2).

Prior to seeking information pursuant to paragraph (1) the employing agency shall put the individual on notice that access to such information will be sought. Information shall be disseminated by a criminal justice agency to an appointing official or legislative body pursuant to paragraph (2) or (3) only after that agency has received notification from the appointing official that he is considering the individual for such an appointment or nomination or from the legislative body that the individual has been nominated for the office and that the individual has been notified of the request for the information and has consented, in writing, to its release.

(b) A criminal justice agency may disseminate criminal justice information to an agency of the Federal Government for the purpose of an employment application investigation, or the approval or renewal of a security clearance for access

to classified information, pursuant to Federal statute or Executive order. The Federal agency requesting information pursuant to this subsection shall adopt regulations reasonably designed to insure that if any adverse information is received (1) employment decisions are made only at a supervisory level, and (2) such information is considered as a disqualifying factor only where it is reasonably related to such employment. At the time he files his application, seeks a change of employment status, or applies for a security clearance, the individual shall be put on notice that such an investigation will be conducted and that access to this type of information will be sought.

(c) A criminal justice agency may disseminate criminal record information to federally chartered or insured financial institutions for purposes of employment review.

SECONDARY USE OF CRIMINAL JUSTICE INFORMATION

SEC. 206. (a) Any agency or person obtaining criminal justice information from another agency or person is prohibited from using that information for any purpose not authorized by law or disseminating that information, directly or through any intermediary, to any other agency or person not authorized by law to receive it.

(b) Rehabilitation officials of criminal justice agencies may, with the consent of the individual under their supervision to whom the information refers, represent the sub-

stance of the individual's criminal record or correctional and release information to prospective employers or other persons if the representation is helpful in obtaining employment or health or rehabilitation services for the individual. Copies of such information shall not be disseminated to unauthorized persons or agencies under this subsection.

SECURITY, ACCURACY AND UPDATING OF INFORMATION

SEC. 207. (a) Each criminal justice agency shall adopt procedures reasonably designed to insure—

(1) the physical security of its criminal justice information systems, including special precautions for patrol cars or patrol units having computer terminals,

(2) the continued accuracy of arrest record information and criminal record information in those systems, including the requirement that arrest records or other records of initiation of criminal charges are followed by a record of disposition within ninety days after the disposition has occurred,

(3) that any additional information (including dispositions), corrections in information, or deletions of information pertinent to the original arrest record information or criminal record information furnished, is promptly disseminated to recipients of that information,

(4) the accurate recording of the identity of persons or agencies requesting arrest record information or criminal record information from the system, the purpose for which the information is requested, and the date of the request,

(5) the accurate recording of the sources of arrest record information and criminal record information entered into the system, and

(6) periodic review and audit of compliance with the provisions of this Act.

(b) Procedures adopted pursuant to this section may exempt information entered into a criminal justice information system prior to the effective date of this Act from those provisions of this section that cannot feasibly be applied to such information.

(c) Arrest record information and criminal record information shall be sealed or purged in accordance with the requirements of a Federal or State statute, or an order of a court of competent jurisdiction when appropriate notification is provided by the agency directly responsible for compliance with the order or statute in each instance.

(d) A Federal or State criminal justice agency which is a central repository of arrest record information or criminal record information shall adopt procedures reasonably de-

signed to insure that arrest record information is expunged when (1) five years have elapsed from the date of the arrest, (2) there has been no subsequent arrest during the five-year period of the same individual, and (3) the individual is not a fugitive.

ACCESS BY INDIVIDUALS FOR PURPOSE OF CHALLENGE

SEC. 208. (a) Upon satisfactory verification of his identity, any individual may inspect, in person or through counsel, arrest record information and criminal record information maintained by a criminal justice agency concerning him, for the purpose of correction, in accordance with procedures adopted by the criminal justice agency.

(b) Each criminal justice agency shall adopt and publish regulations to implement this section, which regulations shall provide—

(1) a reasonable time, place, and procedure to be followed by an individual or his counsel in gaining access to arrest record information and criminal record information, and reasonable fees therefor;

(2) that if, on the basis of the inspection of such information, the individual believes such information to be inaccurate, incomplete, or maintained in violation of this Act, he shall have a right to challenge such information in writing and, if there is no factual controversy

concerning the allegations in the individual's challenge, the criminal justice agency maintaining the record shall expeditiously correct the record;

(3) that if there is a factual controversy concerning the allegations in the challenge, the agency shall refer the challenge to the agency responsible for entering the information for a determination of the validity of the allegations and, if the latter agency finds that there is a bona fide controversy it shall, upon written request of the individual, provide a hearing on the challenge at which the individual may appear with counsel, present evidence, and examine and cross-examine witnesses;

(4) that any information found after hearing to be inaccurate, incomplete, or improperly maintained shall be appropriately corrected or deleted;

(5) that records shall be kept, and provided upon request to the individual, concerning the name and authority of all noncriminal justice agencies to which, and the date on which, such information was disclosed;

(6) that corrections in the information will be automatically transmitted to all agencies which are recorded as having received copies of that information prior to the correction.

(c) No individual who obtains information concerning

himself, in accordance with this section, may be required to show or transfer copies of that information as a condition of employment, licensing, or other regulatory measure to any other person or any other governmental or nongovernmental agency or organization.

CRIMINAL JUSTICE INTELLIGENCE AND INVESTIGATIVE INFORMATION

SEC. 209. (a) Criminal justice intelligence information and criminal justice investigative information may be collected by a criminal justice agency only for official purposes. It shall be maintained in a physically secure environment and shall not be included in arrest record information or criminal record information files.

(b) A criminal justice agency shall adopt internal operating procedures designed to insure—

(1) access to criminal justice intelligence information and criminal justice investigative information within the agency is limited to those officers or employees who require it for the performance of their official duties,

(2) dissemination of criminal justice intelligence information and criminal justice investigative information to other agencies is limited to those officers and employees within the agency who require it for the performance of their official duties and records are maintained for a minimum of three years regarding such dissemina-

tion, including the identity of the agency and persons within the agency to whom it was disseminated, the date of dissemination, and the purpose for which disseminated unless otherwise apparent.

(c) Direct terminal access to automated criminal justice intelligence information or criminal investigative information shall not be permitted outside the agency which stores such information except where authorized by Federal or State statute or Executive order. This subsection does not limit the lawful exchange of criminal justice intelligence information or criminal justice investigative information among agencies within a single executive department by means of an automated criminal justice information system designed for the use of those several agencies.

(d) Criminal justice investigative and criminal justice intelligence information may be made available pursuant to Federal or State statute, or a rule or order of a court of competent jurisdiction.

(e) An assessment of criminal justice intelligence information or criminal justice investigative information may be provided to any individual when necessary to avoid possible danger to persons or property.

(f) A person is guilty of a misdemeanor if, in knowing violation of a specific duty imposed upon him as an officer or employee or former officer or employee of a governmental

agency by statute, or by a regulation, rule, or order issued pursuant thereto, he discloses criminal justice intelligence information or criminal justice investigative information, to which he has or had access in his official capacity, to a person not authorized by law to receive such information. The offense shall be punishable by imprisonment not to exceed one year, a fine not to exceed $10,000, or both.

## TITLE III—ADMINISTRATION AND ENFORCEMENT

### COMMISSION ON CRIMINAL JUSTICE INFORMATION

SEC. 301. (a) There is hereby established in the executive branch of the Government a Commission on Criminal Justice Information (hereinafter the "Commission").

(b) The Commission shall be composed of nine members. Three of the members of the Commission shall be representatives of Federal criminal justice agencies designated by the President. The remaining six members of the Commission shall be appointed by the President by and with the advice and consent of the Senate. Four of the appointed members shall be representative of State or local criminal justice agencies and the other two shall be representative of the public at large. Not more than five of the members at any one time shall be of the same political party.

(c) The President shall designate a Chairman and

Vice Chairman who shall act as Chairman in the absence or disability of the Chairman, or in the event of a vacancy in that office.

(d) Designated members of the Commission shall serve at the will of the President. Appointed members shall serve for a term of three years except that of the members first appointed, two shall be for a term of one year, two for a term of two years, and two for a term of three years. A member whose term has expired shall serve until his successor is appointed. Any vacancy in the Commission shall not affect its powers but shall be filled in the same manner in which the original appointment or designation was made.

(e) Five members of the Commission shall constitute a quorum.

POWERS AND DUTIES

SEC. 302. (a) The Commission shall have the power to—

(1) study and collect information concerning (A) the security, confidentiality, and accuracy of arrest record information and criminal record information, and (B) the compliance of criminal justice agencies with the provisions of this Act;

(2) appraise the laws, policies, and practices of Federal, State, and local governments with respect to criminal justice information systems;

(3) investigate allegations, made in writing and under oath, that there has been a failure to comply with the provisions of this Act; and

(4) require from each criminal justice agency information necessary to compile a directory of criminal justice information systems subject to this Act and publish annually a directory identifying all such systems and the nature, purpose, and scope of each.

(b) The Commission shall report annually to the President and to the Congress with respect to compliance with this Act and concerning such recommendations as it may have for further legislation.

(c) The Commission may submit such interim reports and recommendations as it deems necessary to the President or to the chief executive of any State.

HEARINGS AND WITNESSES

SEC. 303. (a) The Commission or, on authorization of the Commission, any subcommittee of three or more members may hold such hearings and act at such times and places as necessary to carry out the provisions of this Act. Hearings shall be public except to the extent that the hearings or portions thereof are closed by the Commission or a subcommittee thereof in order to protect the privacy of individuals or the security of information protected by this Act.'

56-833 O - 75 - 10

(b) Each member of the Commission shall have the power and authority to administer oaths or take statements from witnesses under affirmation, at hearings of the Commission or any subcommittee.

(c) A witness attending any session of the Commission shall be paid the same fees and mileage paid witnesses in the courts of the United States. Mileage payments shall be tendered to the witness upon service of a subpena issued on behalf of the Commission or any subcommittee thereof.

(d) Subpenas for the attendance and testimony of witnesses or the production of written or other matter, required by the Commission for the performance of its duties under this Act, may be issued in accordance with rules of procedure established by the Commission and may be served by any person designated by the Commission.

(e) In case of contumacy or refusal to obey a subpena any district court of the United States or the United States court of any territory or possession, within the jurisdiction of which the person subpenaed resides or is domiciled or transacts business, or has appointed an agent for the receipt of service of process, upon application of the Attorney General of the United States, shall have jurisdiction to issue to such person an order requiring such person to appear before the Commission or a subcommittee thereof, there to produce pertinent, relevant, and nonprivileged evidence

if so ordered, or there to give testimony touching the matter under investigation; and any failure to obey such order of the court may be punished as contempt.

(f) Nothing in this Act prohibits a criminal justice agency from furnishing the Commission information required by it in the performance of its duties under this Act.

COMPENSATION OF MEMBERS

SEC. 304. (a) Each member of the Commission who is not otherwise in the service of the Government of the United States shall receive a sum equivalent to the compensation paid at level IV of the Federal Executive Salary Schedule, pursuant to section 5315 of title 5, prorated on a daily basis for each day spent in the work of the Commission, and shall be paid actual travel expenses, and per diem in lieu of subsistence expenses when away from his usual place of residence, in accordance with section 5703 of title 5.

(b) Each member of the Commission who is otherwise in the service of the Government of the United States shall serve without compensation in addition to that received for such other service, but while engaged in the work of the Commission shall be paid actual travel expenses, and per diem in lieu of subsistence expenses when away from his usual place of residence, in accordance with sections 5701, 5702, and 5704–5708 of title 5.

DIRECTOR AND STAFF

SEC. 305. (a) There shall be a full-time staff director for the Commission who shall be appointed by the President by and with the advice and consent of the Senate and who shall receive compensation at the rate provided for level V of the Federal Executive Salary Schedule, pursuant to section 5316 of title 5. The President shall consult with the Commission before submitting the nomination of any person for appointment as staff director. Within the limitation of appropriations, the Commission may appoint such other personnel as it deems advisable, in accordance with the civil service and classification laws, and may procure services as authorized by section 3109 of title 5, but at rates for individuals not in excess of the daily equivalent paid for positions at the maximum rate for GS–18 of the General Schedule under section 5332 of title 5.

(b) The Commission may constitute and fix the duration of advisory committees within States composed of citizens of that State and may consult with Governors, attorneys general, and other representatives of State and local governments, and with private organizations as it deems advisable.

(c) Members of the Commission and members of advisory committees constituted pursuant to subsection (b) of this section, shall be considered "special government em-

ployees" within the meaning of section 202 (a) of title 18, notwithstanding the number of days actually employed in the work of the Commission.

ADMINISTRATIVE SANCTIONS

SEC. 306. Each criminal justice agency shall adopt procedures reasonably designed to insure—

(a) that its personnel are advised of the provisions of this Act and of disciplinary actions that may be taken for violations of this Act or procedures established thereunder;

(b) that other agencies receiving access to information pursuant to this Act are notified that misuse of information obtained may subject them to administrative sanctions including the termination of any future access; and

(c) that other persons receiving access to information pursuant to this Act are notified that misuse of information obtained may result in the denial of future access to information.

JUDICIAL REMEDIES

SEC. 307. (a) An individual who is denied access to information concerning him in violation of section 208 or who seeks review of a final agency decision refusing to correct or delete information as provided in section 208 may bring a civil action against the responsible agency.

(b) An individual with respect to whom information has been maintained, disseminated, or used in violation of this Act or implementing procedures of an agency may bring a civil action against the individual or agency responsible for the alleged violation. If relief is sought against both an individual and an agency responsible for the alleged violaton, such relief shall be sought in a single action.

(c) (1) If a defendant in an action brought under this section is an officer or employee or agency of the United States, the action shall be brought in an appropriate United States district court.

(2) If the defendant or defendants in an action brought under this section are private persons or officers or employees or agencies of a State or local government, the action may be brought in an appropriate United States district court or in any other court of competent jurisdiction.

(d) The district courts of the United States shall have jurisdiction over actions described in this sanction without regard to the amount in controversy.

(e) A prevailing plaintiff in an action brought under this section may be granted equitable relief, including injunctive relief, and actual damages, and may be awarded costs and reasonable attorney fees. In appropriate cases, a prevailing plaintiff may also be awarded exemplary damages.

(f) Good faith reliance upon the provisions of this Act

or of applicable law governing maintenance, dissemination, or use of criminal justice information, or upon rules, regulations, or procedures adopted by an agency in implementation of this Act or other applicable law, shall constitute a complete defense to a civil damage action brought under this section but shall not constitute a defense with respect to equitable relief.

(g) Nothing in this Act or in any regulations or procedures adopted pursuant thereto shall provide the basis for the exclusion of otherwise admissible evidence in any proceeding before a court, parole authority, or other official body.

CONSENT TO SUIT

SEC. 308. Any State or local agency which operates or participates in a criminal justice information system subject to this Act shall comply with the provisions of this Act and shall be deemed to have consented to the bringing of actions pursuant to section 307.

EFFECT ON STATE LAW

SEC. 309. Nothing in this Act is to be construed as diminishing greater rights of privacy or protection provided by a State law or regulations governing use, or updating of criminal justice information within that State. Use of information in interstate systems or the use of information obtained through interstate transfer shall be governed solely by this Act.

APPROPRIATIONS AUTHORIZED

SEC. 310. There are hereby authorized to be appropriated such funds as are necessary for the purpose of carrying out the provisions of this Act.

REPEALER

SEC. 311. The second paragraph under the heading entitled "FEDERAL BUREAU OF INVESTIGATION; SALARIES AND EXPENSES" contained in the Department of Justice Appropriations Act, 1973" is hereby repealed.

EFFECTIVE DATE

SEC. 312. The provisions of this Act shall take effect upon the first day of the twenty-fifth month following the date of enactment, except that sections 301 through 305 and section 310 shall be effective immediately.

Senator TUNNEY. I am very pleased to be able to call to the witness stand Attorney General Francis X. Bellotti, the attorney general of the State of Massachusetts.

Mr. BELLOTTI. Chief Pomerance has to catch a plane. He has 15 minutes. So I defer to him.

Senator TUNNEY. Certainly.

## TESTIMONY OF ROCKY POMERANCE, POLICE CHIEF, MIAMI BEACH, FLA., AND PRESIDENT OF THE INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

Mr. POMERANCE. Thank you.

Mr. Chairman, I am Rocky Pomerance, chief of police of Miami Beach, Fla., and president of the International Association of Chiefs of Police. I appear here today at the direction of the executive board of the IACP, which unanimously endorsed this statement.

As spokesman for IACP, I should point out that IACP is the world's leading association of police executives. We have over 10,000 members drawn from every State in the Union and from over 60 other nations.

Throughout our 82 years of existence, we have consistently pressed for the upgrading and professionalization of police services. Especially during the last decade we have undertaken or supervised a wide range of research and training programs. Since we have such a broad constituency, we feel we can speak truly for the needs and concerns of the entire law enforcement community.

The vast majority of police departments are opposed to any form of legislation similar to Senate bill 2008. The members of IACP are aware that the American public has become concerned about the power which may be improperly wielded by Government agencies straying beyond the bounds of their proper missions.

Indeed we in the law enforcement community have long been aware of the fact that intensive intelligence and investigative operations and the maintenance, use, and dissemination of criminal justice information present potential threats to individual rights.

It is because of this very awareness that law enforcement agencies have severely restricted access to files and have instituted strict security measures with regard to all forms of criminal justice information, intelligence information, and investigative information.

Although a few criminal justice agencies have not established strict procedures and may have overestimated the needs of law enforcement in relation to individual rights, the existence of these few situations does not mandate Federal legislation imposing stringent standards on all State and local agencies.

Indeed, despite the recent public focus on privacy and intelligence operations, there have been few substantiated reports of violations committed by State and local law enforcement agencies.

Passage of Federal legislation at the present time would constitute a failure by the Federal Government to recognize the fact that criminal justice agencies have been headed by officials who have taken actions deemed necessary to protect individual rights of privacy and have not intentionally violated these rights.

The fact that few States have enacted comprehensive statutes addressing the criminal justice information and intelligence areas

should not lead to a conclusion that the Federal Government needs to legislate. Few States have addressed all the ramifications of this problem, because it is only recently that the public and the legislators have come to realize the scope of problems presented in the privacy field. The Federal Government, likewise, has only recently given attention to this field.

The Federal Government has consistently recognized, and should continue to recognize, the right and ability of the States to legislate in the field of law enforcement. One of the cornerstones of the American democracy has been the absence of national control over the police.

Throughout our 200 years of experience, we as a Nation have opposed Federal control over State and local police, and no matter how well intentioned the purposes motivating the Federal legislation.

This tradition of the autonomy of State and local police has arisen from a recognition of the people's need to have control over the police exercised by those governmental bodies closest to them—the States and the localities.

By taking yet another step toward national control over the police, we are actually further endangering individual rights.

Essentially we believe that S. 2008 unnecessarily imposes upon State and local agencies standards dictated by the Federal Government, which would grant the Commission the ability to control the day-to-day details of State and local criminal justice administration.

We believe that if any Federal legislation is enacted at this time it should not remove from the States the duty and power to fashion particular standards and procedures to protect individual rights.

A better approach to legislation would be to differentiate between systems involving only State and local agencies and those addressing Federal or joint State-Federal systems with Federal legislation only as to the latter.

Proper legislation should not dictate the particular standards or procedures to be adopted by systems maintained or used solely by State and local agencies. Rather it should confine itself to the enunciation of certain general goals to be accomplished by State and local agencies. This method would leave to the States the duty to define the rights of individuals in the privacy field.

The Federal Government might be helpful by studying problems arising in this field and by drafting model statutes, rules and regulations, and presenting these models to the various State and criminal justice agencies for consideration. The States and criminal justice agencies would not be forced to adopt these models, rather, they could fashion whatever standards or procedures they deemed best suited to meet the general goals.

If there is to be Federal legislation, it should more properly contain certain minimum standards to be followed by the Federal criminal justice information systems, and provide for only that rulemaking power deemed necessary to apply these standards to State-Federal or purely Federal exchanges of criminal justice information.

In order to assure that this rulemaking does not conflict with the right of States to regulate their own systems, this rulemaking power should not be extended to the procedure of State and local criminal justice agencies with regard to any information not obtained from the Federal system.

Unfortunately S. 2008 is not only an intrusion by the Federal Government into a field traditionally left to the States; it is a restrictive measure which would seriously curtail the ability of law enforcement agencies to protect the public.

Discussions related to criminal justice information and the right to privacy have focused on the need to balance three key interests: (1) The rights of privacy of individual citizens; (2) the necessity for law enforcement to utilize the tools needed to protect the public; and (3) the right of the public and the press to be informed.

In our opinion, the balancing of these three key interests has been improperly applied in S. 2008. One key societal interest not directly addressed is the right and need of the public to protection—to be free from crime and the fear of crime.

Focusing on this interest, as well as the other three, leads one analyzing S. 2008 to realize that the effect of the severe restrictions imposed on legitimate activities and procedures of law enforcement agencies will be an unnecessary reduction in the protection afforded the public.

Crime is still a major threat to the American public, and I am certain that the Congress would want to be particularly cognizant of the effects of restrictive legislation like this bill upon the ability of law enforcement to fight crime in America.

If the restrictions imposed in this bill result in the inability of police to detect murderers, rapists, or saboteurs, with the result that those persons remain free to continually commit crimes of violence, the rights of Americans would be unnecessarily endangered.

Unfortunately, the result of this bill as now written, would be that many violent criminals should remain free. To grant such a benefit to organized crime and criminals is much too heavy a price to have society pay.

We have pointed out two key reasons why we believe the bill is unsound: The dangers arising from increased Federal control over law enforcement and increased exposure of the American public to crime, due to the curtailment of law enforcement activities.

These conclusions are based upon a careful analysis of the provisions of S. 2008; specific criticisms of the most significant problems are developed in our written report. Since the subcommittee's time is now limited, we would like to focus on four of the specific provisions in the bill.

Section 208 provides for the sealing and purging of the criminal justice information. These requirements will severely restrict the access of law enforcement agencies to records which have proven highly useful in the past.

The requirements for the sealing or purging of certain arrest record information in the event of nonprosecution are highly unrealistic. The decision not to prosecute may have been based on a tangential matter, such as the exclusion of essential evidence or the decision of the key witness not to testify—as often happens in sex offense cases—or a public attitude opposed to full enforcement of certain laws.

In many cases where the guilt of the arrestee has not been proven, the arrest and criminal history record information are of proven usefulness.

Another key flaw of section 208(a) stems from the failure of this section to consider the impact of cases where the accused is found not

guilty because of insanity, or is not prosecuted because of his mental incompetence. In such cases, the defendant is usually civilly committed and must undergo psychiatric therapy and counseling. If a literal reading of section 208(a) were employed, criminal justice information would have to be sealed, even while the individual was still civilly committed.

As another example of the difficulties created by the broad scope of section 208(a), consider the problems faced by law enforcement agencies in their battle against organized crime. If the sealing and purging requirements of this section were put into effect, only 39 of the 282 records relating to the Gambino crime family would be unsealed. The same problem would exist as to almost all underworld leaders.

Section 308 is one of the key provisions of the bill. It allows an aggrieved person to bring a civil action for violation of the act or regulations promulgated pursuant to it. It is a sweeping damage remedy, which allows the successful plaintiff to recover, at a minimum, liquidated damages, attorneys' fees, and costs.

It also provides for exemplary and punitive damages, as well as injunctive relief. The only defense provided is the good faith reliance upon the assurance of another agency or employee. This defense is unquestionably too narrow. In contrast, the Justice Department bill provided that one's own good faith interpretation of the act or implementing rules, regulations, and procedures would be a complete defense.

By allowing only a narrow ground of defense, S. 2008 will punish officers for their good faith mistakes. The threat of such punishment will in turn result in a chilling effect upon law enforcement efforts in any situation which might arguably violate the act or rules and regulations. Thus a realistic result of section 308 will be to multiply the restrictive effects of all the other provisions of the act.

Enforcement of S. 2008 would be through a joint State/Federal Commission on Criminal Justice Information to be established pursuant to section 301. Our earlier testimony has pointed to many of the problems presented due to the pervasive powers in the administration of S. 2008.

There is another basic conceptual deficiency in the Commission on Criminal Justice Information. This section provides no assurance that the Commission will be properly representative of the interests primarily affected by this bill. The key impact of this legislation would be upon State and local law enforcement agencies. S. 2008 does not assure that Commission members drawn from the State and local criminal justice agencies will be truly representative.

For instance, under S. 2008, the seven members from State and local agencies could all be from one component of the criminal justice system, or from one region of the Nation. In order to assure that the Commission would properly reflect the groups affected by this legislation, we would suggest a commission composed of both Presidential appointees—subject to Senate approval—and members appointed by organizations representative of the various criminal justice agencies.

As a specific example, we would propose a 17-member commission. The Attorney General, the two other Federal agency officials, and two representatives of the public at large would still be Presidential appointees.

In addition, we would suggest that the President be allowed to appoint five members drawn from different size police departments: one member from a department with less than 100 employees, one from a department with between 500 to 1,500 employees, one from a department with more than 1,500 employees, and one from a State police agency.

These five representatives would have to be from five different States in various regions of the Nation and would be subject to Senate confirmation.

In addition to these 10 Presidential appointees we would suggest that 7 organizational representatives be added to the Commission. These members would either be directly appointed by organizations they represent or chosen by the President from a list of candidates submitted then by each organization.

In order to assure diverse representation, we would propose that the range of the seven organizations be similar to the following: 1. Project SEARCH, 2. National District Attorneys' Association, 3. International Association of Chiefs of Police, 4. the Judicial Conference of the United States, 5. the National Conference of Criminal Justice Planning Administrators, 6. the National Sheriffs Association, and 7. the Professional Corrections Association.

This type of distribution will assure that the Commission receives direct input by the State and local agencies most closely affected by this legislation. Furthermore, the 5-year duration of the Commission should be modified so that the Commission would continue as long as the act remains in effect.

This would assure that State and local agencies would continue to have a voice now in the administration of the act.

Long experience has shown that many of the key policy decisions of a commission, whose members meet only occasionally are not made by the commissioners, but by their professional staff. Section 306 of S. 2008, by making the staff director a Presidential appointee, fails to recognize this reality.

This bill should include a provision whereby the Commission can either choose the staff director or submit to the President a list of nominees. Such a provision would assure the Commission direct control over the staff director; then otherwise the State-Federal Commission might be little more than an advisory body to the full-time professional staff located in Washington.

In conclusion, sir, the IACP is opposed to S. 2008 in its present form because of its severe restrictions on the ability of law enforcement to fight crime and the encroachment by the Federal Government on the traditional role of the States in the field of criminal justice.

Although the individual's right to privacy is essential and is respected by law enforcement, consideration of the right to privacy must not unduly impede State and local law enforcement's fight against crime.

Thank you for giving me the opportunity to present the views of police executives across the Nation.

Senator TUNNEY. Chief Pomerance, do you have 5 minutes?

Mr. POMERANCE. Yes.

Senator TUNNEY. First, I thank you for being here and I know you made a great effort to be here. I have a few quick observations before I ask you two or three questions. I am impressed by your critique of the

Commission, particularly the need for specifying and expanding its membership and making it survive as long as the underlying legislation is the law.

I would appreciate any additional thoughts you have along those lines. However, I find it difficult to believe that you and others are unaware of the abuses that have taken place in the past few weeks and months, which have led to this legislation and those originally introduced by Senator Ervin 4 years ago.

Two weeks ago I asked the Library of Congress to compile a list of the intelligence information from the State and local levels since the beginning of the year. Yesterday the Library sent me a file of clippings that must weigh several pounds.

As a matter of fact, just the index of the clips fills six single spaced pages. I would like to emphasize that the Library only had limited time, used only a dozen or so big city newspapers and was restricted to only State and local intelligence abuses.

Yet they were still able to compile this incredible record of materials. I recognize that there is a genuine concern on the part of the local law enforcement officials that they are going to have the Federal Government dictate to them what has to be done in the way of establishing law enforcement systems at the local level.

As I mentioned in my statement, it is our desire to prevent that. We do not want to create a national police force. We do not want any agency to ration out information to local law enforcement agencies or tell them what they have to do or what they may not do.

You have made a heavy criticism of S. 2008 as an unwarranted intrusion. Yet this bill requires the States to legislate their own priorities in the criminal justice matters and gives the dominant voice to State and local officials in the regulation of criminal justice information through the mechanism of the Commission.

I find it difficult to reconcile your statements that this is going to be a dominant Federal intrusion into local and State law enforcement activities when one reads in the bill that such a clear priority has been given to State and local governments in the establishment of the Commission and in the policies which will be laid down by the Commission.

Mr. Pomerance. Insofar as the collection of abuses, those alleged violations, few or any have been substantiated in any final proceedings. These are newspaper accounts. While we are discussing the media, it would appear that although the police are denied access to arrest information of specific nature, the news media have their morgues and we could be going to the newspaper morgues to get our information which we need to operate.

There seems to be an unhealthy dichotomy here and I have some concern how this is going to affect the press, as well, by the way although I am certain they can speak for themselves when their opportunity comes to discuss this with you.

Insofar as calling it to the attention of the police on the local-State level, I am always mindful of the mule skinner who hit the mule with a 2 by 4 and indicated it was just to get his attention. This is like dropping a nuclear bomb on us and telling us it is to get our attention to improve.

I don't believe that we would ask a carpenter and a plumber to build a building and then deny them a saw and a hammer and nails

and a wrench. Some of the revisions in here—and I know how well intentioned they are because I have a personal high regard for privacy of the individual and have displayed that throughout my own career—will have this chilling effect that ultimately, I sincerely believe, will work to the detriment of the public.

We are really not a separate body. We are an extension, we are the people's surrogate. We are an extension of the people's authority. So when this is denied the law enforcement I am afraid that the public ultimately will be the casualty.

Senator TUNNEY. One of the things that we do have is a difference of opinion on the part of local law enforcement officials as to the impact of this legislation.

Right after you leave the witness stand we are going to hear from a State official who is going to testify that this bill will not hinder effective law enforcement. I know also from the study this committee has done that most of our equivalent Western European countries have much stricter privacy safeguards on this kind of information than we do.

I find it difficult to believe that stale and inaccurate and incomplete law enforcement information has any value. I don't see how, if it is inaccurate, or if it is incomplete, or if it is old and stale and thereby not relevant, that it does have value.

That is one of the things we are trying to address in this legislation, to prevent that kind of information from being used against a person wittingly or unwittingly.

Just pick up the Washington Post today, and you see a big headline, "Kelley Affirms That FBI Broke In." Some people call those rumors. I recognize that the reality of a situation is dependent upon the point of view of the individual, and I am sure that from the point of view of the FBI officials who authorized those break-ins that it was good law enforcement.

On the other hand I have a feeling that a judge in the case would have said that, under the criminal statute, there had been a burglary committed.

I feel that we must protect society against those uses of information, inaccurate criminal data in the hands of malevolent people, people who are not conscientiously trying to do the job that society is paying them to do, who are, in other words, breaching their public trust.

We want to protect people against the law enforcement officials who may decide that at a given point in time they are not going to abide by the regulations in the law. That applies at the Federal level as well as at the local level.

I strongly feel that law enforcement should be left wherever possible to the State and local agencies, and I am opposed to the expansion of the power of any central law enforcement agency at the Federal level because of the potential for violation.

But I don't see how you can say that the keeping of inaccurate and incomplete information by local law enforcement agencies has value.

Mr. POMERANCE. Senator, you have referred to inaccurate and incomplete information and I share that concern.

All professional police share that concern because it is useless to us. We are not speaking of inaccurate and incomplete information. We are speaking of accurate and complete information.

We can't use the abuse by one individual who has not performed properly, and point to his particular abuse at a local level and say, "There it is, that is law enforcement in America."

I think after listening to you, Senator, that you and I, just as the police and the Congress, are truly searching for an appropriate answer. It is a method by which the interests can be balanced out without having the baby go out with the dirty water.

I grant you that it is a difficult task. What I would ask is that we have an opportunity to work further toward this type of legislation and perhaps we can mutually come up with something more appropriate that will protect the individual's right to privacy and yet not destroy his right to walk on the streets of American cities.

The quality of life in America is deteriorating because of that. I know from listening to you and reading your statement that obviously, you share the same concern.

Senator TUNNEY. Thank you very much, Chief. I know you have a plane to catch. We are grateful for your taking the time to testify.

Our next witness is the attorney general from the State of Massachusetts, Francis X. Bellotti. I understand he is going to be introduced by Senator Kennedy.

## STATEMENT OF HON. EDWARD M. KENNEDY, A U.S. SENATOR FROM THE STATE OF MASSACHUSETTS

Senator KENNEDY. Thank you very much, Mr. Chairman. I appreciate the opportunity as a member of this committee and a supporter of the legislation to present to this committee our distinguished attorney general of the State of Massachusetts. Attorney General Bellotti has been a distinguished lawyer and a great friend, and beyond that has been one of the most effective and articulate spokesmen for the rights of privacy, as well as a hard-hitting and effective law enforcer.

I know, Mr. Chairman, that you have given a great deal of time and attention to the issue of the right of privacy. This subcommittee which you chair has been concerned about privacy for over 10 years, and you certainly appear to be a worthy successor to the distinguished Senator from North Carolina in your pursuit of this particular issue.

As you are applying the various lessons and warnings in the whole area of crime and criminal law, I can testify that in the whole health area, for example, we have similar kinds of issues. Any individual in this country who applies for health insurance, for example, whether he is in San Diego or Boston, files information which goes into a great computer. Anytime after that you can push a button and out comes a printout whether they have heart disease or some kind of genetic disease. And this information, which is often outdated or simply erroneous, may be made generally available to all of the major insurance companies in this country.

They can, in looking through that data, get the most sensitive, confidential information that one can possibly imagine. You are right—certainly in the particular area which we are considering today, in the area of criminal history information—to target your concern on the whole privacy issue.

I don't think any of us doubt the importance in law enforcement of accurate, detailed, timely information. On the other hand, information that is inaccurate or hearsay or without substance or substantiation, not only fails to serve the interest of law enforcement, but also violates in the most important way the right of privacy of individuals.

I am proud that on this opening day of hearings that this subcommittee has a spokesman from Massachusetts. As you know, Mr.

Chairman, in 1972 Massachusetts passed the criminal offenders and record information law which set up a rather elaborate procedure, sensitive to the kind of issues which you are concerned about here today.

Our attorney general, Francis Bellotti, has, since the time he has been the attorney general, demonstrated what an attorney general can do in enforcing the laws of the Commonwealth of Massachusetts while fully sensitized to the rights of privacy of each citizen of our State.

I think the experience of that State, and of our attorney general, reflecting a deep concern and awareness and commitment to both law enforcement and right to privacy, can be enormously beneficial and valuable to this committee. I am delighted he has been willing to come down and share his experiences with us and with the committee.

Senator TUNNEY. Thank you for the warm introduction of our next witness. I want to thank you, Senator, for the work you have done in this area. As a member of this subcommittee over the years—you were on the subcommittee before I was on the Judiciary Committee—I know that you have taken a great interest in this matter.

I hope we are going to be able at long last to move this legislation through the Congress; at least through the subcommittee, where we have some degree of control over what the final product will contain.

We have delayed too long. You point out so accurately how the most private, personal data from health records can be made available to insurance companies by turning over computerized forms to them. These insurance companies Xerox the data and turn them over to others who have absolutely no reason or right to know the medical history of an individual.

In this particular case we are dealing with criminal records. In talking to law enforcement officials who are deeply concerned about rights of privacy and also about apprehending criminals and protecting society, I find that much of the information contained in criminal records, particularly intelligence records, is inaccurate, incomplete, and stale to the extent that it does not serve a useful purpose, where they are looking for suspects, in connecting an individual with a crime that has been committed.

I want to thank you very much for your interest in the legislation and for giving such a warm endorsement to our next witness.

## TESTIMONY OF HON. FRANCIS X. BELLOTTI, ATTORNEY GENERAL, THE STATE OF MASSACHUSETTS, ACCOMPANIED BY JON BRANT, ASSISTANT ATTORNEY GENERAL, AND ANDREW KLEIN, SPECIAL ASSISTANT TO THE ATTORNEY GENERAL

Mr. BELLOTTI. I want to thank you, Senator Kennedy, for coming here to introduce me.

One of the things that I would like to say before I begin my remarks on S. 2008, which I favor in a general sense, is that I have for a long time before my election served as Lieutenant Governor of Massachusetts, and I have defended probably 2,000 cases in the courts, Commonwealth and others, so I suppose I am very sensitive to this particular issue from both sides, from having defended cases and from being the law officer in my State.

I think that this is probably the most significant issue of maybe the next 6 or 7 years. The thing that would most logically affect the

rights of the people of this country in the most acute way, the most dangerous part of the issue is that people seldom get concerned about privacy until it affects their lives in a particular and specific way.

In this issue, one of the dichotomies you can see is your exchange with Chief Pomerance. You both want to come out the same way. Law enforcement officers feel that privacy is inimical to law enforcement. The Governor who has preceded our present Governor had a great concern.

I have two of his people, Andrew Klein and Jon Brant, who have both devoted their lives to this particular issue and have done a great deal in our State to accomplish what we have accomplished.

I am not going to reiterate the Governor's testimony but I would indicate a shared conviction: The danger our democracy faces is not so much the specific outrages of future Watergates, but the continued and persistent encroachment by executive government agencies into the affairs of the States, and ultimately into the private lives of every one of us.

I just argued the oil import license fee before the circuit court of appeals yesterday. The thread that seems to run through both these issues is that Federal agencies, the Federal Bureau of Investigation included, have a tendency to almost excuse everything in the name of national security, things of that nature.

Executive orders seem to be so flexible that we have great difficulty protecting individual liberties under them. I think that nowhere is the threat to our democracy greater than the area of Federal criminal justice information systems, including the FBI's National Crime Information Center's computerized criminal history program and related manual identification files.

Massachusetts has refused to participate in NCIC, the FBI's computer, but all States send those manual rap sheets, fingerprints, down to the FBI. Presently those would be included in the big computer which means that even though we refuse to go into it or participate in NCIC because of manual files going in, they become part of the central system and not susceptible to controls that we have and the standards that we have in Massachusetts.

To indicate how far we have come down this dangerous road, one has only to go back to the turn of the century when central registries of fingerprints were first established. At that time fingerprints on persons found not guilty were returned to their subjects.

Today the FBI's identification division has some 200 million fingerprints including files on millions of individuals never even arrested for a crime.

Sixty years ago when Congress first debated the establishment of the FBI, one of the great concerns, the single most expressed fear again was that such a Federal police force might someday adopt practices habitual to other countries. Congress was concerned that such an agency might someday engage in such practices as the collection and lodgment in police files of rumors, suspicions, and gossip, as well as information about the private lives of persons who were not criminals.

Today precisely this has happened. This type of information has been computerized and it is susceptible to dissemination all over the country. Once inaccurate information gets into this tremendously complex and integrated system of computer data banks, it is irretrievable. There is no way you are ever going to bring this back.

Today such information is computerized and disseminated around the country in microseconds.

Never before had they had regulations. Regulations have emanated. If you look at the regulations you will see that there are a great many things wrong with the FBI regulations. We are contemplating instituting suit to enjoin the effectiveness of these Department of Justice regulations.

I believe that what they do is computerize and institutionalize and formalize a great many of the constitutional deficiencies that had been built in a very loose way into the operations of the Department of Justice.

Finally one has only to look back 2 months, to May 20, and examine the new Justice Department regulations for criminal justice information systems to realize that this dangerous trend is accelerating.

Mr. Chairman, these regulations are unequivocal evidence of the Justice Department's unwillingness or its inability to regulate itself and prevent further encroachment of 10th amendment rights of the States and the basic constitutional rights of every citizen.

These regulations are a compelling testimony for the urgent need of legislation like that before us today. The regulations are totally inadequate. They do little more than codify existing inadequacies and lack of control over current Federal criminal justice systems. Worse they help insure these systems become more intrusive and abusive.

The two major new problems, as I see them, among many, many others, are:

1. By defining manual identification fingerprint arrest rap sheets as part of the NCIC, these regulations permit the FBI to computerize existing manual files for inclusion into the NCIC/CCH over the specific objections of States, such as Massachusetts, Pennsylvania, and New York, which have refused to participate in the NCIC/CCH. The result is to magnify the potential abuse of this system by a factor of 40 (from one-half million records to 20 million records).

2. These regulations also pave the way for the FBI to control to an extent previously unimagined, local police activities by controlling police telecommunications, and they can control and monitor conversations with police departments throughout the system. This would be again an encroachment upon the powers of the individual States.

The further down this road we go the more we have to understand that the acquisition and control of information is the acquisition of power, the acquisition of control over the lives of our citizens.

I think more than any other mechanical aid, the collection, dissemination, storing, categorizing, and giving access to information is what may very well affect either the erosion or the persistence of democratic form of government.

Far more than cannons or rifles or anything else, information has become the greatest weapon in the free world. We have to look at that very carefully or we will have arrived in 1984 in 1975.

I have been able to persuade a great many of them that privacy is very consistent and very parallel with individual liberties. A great many police officers are finding this out in this country when they find that their files become part of a computerized system.

They discover that what they do off duty becomes part of the concern of a police commissioner or a police chief. The police gen-

erally, particularly patrolmen, are becoming very aware of this precise issue.

Mr. Chairman, if the Massachusetts experience shows anything and as you know we were one of the first States to legislate in this area, it is that to control these systems, to insure their effectiveness for law enforcement and privacy, self-regulation by administrative fiat does not work, nor will it ever work, because it is too variable. The standards should be consistent. If we have a government of laws then we are going to have to have a government that operates regardless of the particular ideological bent of the occupant of the office at that particular moment.

That should not be a variable.

The basic mission of a police agency, whether it is the Boston police or the FBI, is to investigate, maintain order, and arrest people. Similarly the basic mission of the courts is to try cases, and the goal of prisons is to rehabilitate criminal offenders. However, none has as a primary goal the collection, maintenance, dissemination, and regulation of complete criminal history records.

Our experience shows that a separate agency must be established whose only mission is to regulate criminal justice information systems. Further, this agency should be established by law. This law should also lay down minimum standards to insure privacy and individual rights. We must remember that privacy and law enforcement are not mutually exclusive.

A major responsibility of the criminal justice system, after all, is to rehabilitate criminal offenders. This becomes impossible if past criminal records, promiscuously disseminated, prevent rehabilitation.

In 1972, Massachusetts passed such a law, which established such an agency called the Criminal History System Board. I now serve as chairman of this agency. Further, our legislation reestablished basic standards to protect the privacy.

Copies of this law have been made available to you so I won't describe it in detail. Generally our law is in agreement with the standards set by S. 2008 with one important exception.

Under our law, access to criminal history records is limited to criminal justice agencies and agencies with specific statutory authority. Unlike S. 2008 access is not allowed by Executive order. This is one of two major weaknesses in S. 2008.

Before I was elected, maybe 133 separate types of agencies all over the country have access, limited access, to our criminal history systems in Massachusetts. We have the licensing board, liquor licensing board, and things of that nature.

I am going to reevaluate all of those and take a hard look and see who has access. If we set high standards in our State for the dissemination of this information, I do not want to see this go out to some other State that has low standards and maybe turning this information over to credit agencies.

All of this can happen depending upon available sets of standards in the 50 States respectively. If you are going to get into the Federal computer, NCIC, if you are going to have Federal intervention at all, then the Government should set a set of very high standards to which the participating States must comply both in putting in information and giving access to information.

Short of this, I can assure you that Massachusetts will never participate in any Federal computer, NCIC or anything else. There is no way we would do this. As a matter of fact we would resist it by bringing suit against the Department of Justice in this area.

For example, the Governor of our State cannot gain access to these files, except for consideration of a specific record of a person before him for a pardon.

Our insistence on statutory authority only has proven to be amply justified over the past 2 years. Let me explain, with some recent history. After chapter 805 went into effect in 1972, Massachusetts was sued by the Justice Department in Federal district court, on behalf of the Small Business Administration, the Defense Investigatory Services, and 75 other Federal agencies denied access under this provision.

Although these agencies did not have any congressional authorization for access, they all alleged that access was essential for a variety of reasons, including in the case of the Defense Investigatory Services, national security.

That was the area into which they moved very, very shortly. The case was finally dropped by then U.S. Attorney General Elliot Richardson. None of these agencies, to this day, receive these records they then alleged to need so desperately. But as far as I know, all continue to operate effectively in the Commonwealth of Massachusetts. The Small Business Administration still gives out loans. Massachusetts citizens still are employed in defense related projects.

So there is really not the need to know that everyone likes to believe there is.

There is another moral, too. Although the Defense Investigatory Services alleged it needed these records for national security, it did not and does not get them, and top secret Government research is still conducted at the Lincoln Lab at MIT. The national security has not been imperiled.

If anything I suppose recent disclosures concerning the Defense Investigatory Services, and its immediate predecessors, suggest that these agencies may have violated State and Federal law by snooping into private lives of citizens. Perhaps they themselves were the real threat to the security of our democracy.

Doesn't national security mean the preservation of the democracy as it exists?

Senator HRUSKA. Will the witness yield? There is a vote in process, Mr. Chairman.

Senator TUNNEY. We will have to recess for a few minutes so that we can go over and vote and come back.

Senator HRUSKA. Before we do, I would like the record to show that I know the sincerity of the chairman and I am aware of his desire to accommodate the witnesses, but this meeting is being held in violation of the rules of the Senate.

I regret very much to point out, Mr. Chairman, that these hearings are in process at a time when they are forbidden, and I believe we should be cognizant of the rules of the Senate.

May I say further for the record the reason for this rule is the pendency in the Senate chamber of business of high priority. It is not my decision. There is no reflection at all upon the excellent testimony which the Attorney General has given.

[Voting recess.]

TESTIMONY OF FRANCIS X. BELLOTTI—Resumed

Senator TUNNEY. The subcommittee will come to order. Let the record reflect that whereas the points that Senator Hruska brought up before we recessed, that the subcommittee was considering the Wyman Berkely matter, was correct and we should not have been in session.

Senator Hruska had been here for 10 or 15 minutes and had not raised a point of order, which the Chair would have complied with if he had raised that point of order.

I am sorry about the situation as it has arisen today. One of the reasons that I wanted to go ahead with these hearings is that you had come from Massachusetts. Our other witness had come from Florida to testify. I thought that unless a point of order was raised it was more important to conduct the business of the Senate than to go over and listen to a wrangle on the Senate floor that is accomplishing nothing.

I know you have to catch a plane. I would like you to proceed and finish your testimony and I will submit questions to you in writing so that you can respond.

Mr. BELLOTTI. Thank you very much, Senator. I will be happy to answer any of those questions for you. I had one or two more things. I had just begun to address myself to the telecommunications problem when the hearing recessed.

The other concern besides the executive order provisions of S. 2008 would be its failure to prohibit further Federal intrusion into the area of local police telecommunications. I had touched on the FBI superimposing itself and its system over all of the others, being able to control and monitor State and local telecommunications systems.

I think that this should be handled by legislation and not be left to an appointed commission to act sometime in the future. I wanted to read to you a little bit to indicate the president's telecommunications office on this issue. I would like to quote:

> A growing Federal role in police telecommunications would not only weaken the ability of the other levels of government to manage their own affairs but also raises concerns about the protection of individual rights . . . as we stated to you when we were first appraised of the FBI proposal, we fear that it could result in the absorption of State and local systems into a potentially abusive, centralized, federally controlled communications and computer information system.

Mr. Chairman, with these two exceptions, I believe S. 2008 to be excellent, timely, and crucially important legislation. Passage will help us replace the current highly centralized but loosely controlled Federal system, with a highly decentralized and strongly controlled local and State oriented system.

It is not a total answer but it is the best that you can come up with at the moment. I strongly feel it should be enacted.

The present system remains intolerable. For this reason I am in the process of preparing, with other State attorneys general, a suit to enjoin continued operations of the NCIC/CCH which violate constitutional rights and guarantees.

In response to an initial letter sent to all State attorneys general, 15 shared this concern and only 6 disagreed among those who responded.

I sent a letter to attorneys general throughout the country and received only six letters in opposition to our position and 15 shared this concern very strongly.

I will leave with you copies of our law, chapter 805, and current regulations pursuant to that act. I will also leave copies of our critique of the recent Justice Department regulation governing criminal justice information systems detailing their constitutional and statutory deficiencies.

I would be happy to answer any questions you might have.

Thank you. I very much appreciate your holding the hearing and I am very grateful for the opportunity to come down here and not only express our concerns on this issue but to give you whatever support we can give you from the distance we are to the enactment of this legislation which I feel to be a very important first step.

Senator TUNNEY. I know you have to catch a plane at 12 o'clock so we will submit our questions in writing.[1] But I would like to ask just one more question before you leave.

You do not believe then that this legislation, if passed, would hinder law enforcement officials in pursuing their duties?

Mr. BELLOTTI. Not at all. If they are concerned with a constitutional system of government, I cannot imagine how it could impede law enforcement. Law enforcement does not mean conducting intelligence surveillance, prying into everybody's life, inhibiting conduct and political dissent. It means preservation of our system of government and what differentiates us from every country in the world, the pursuit of individual liberties in the balance with relation to everybody else's rights.

A short answer is no, I do not.

[The prepared statement and exhibits submitted by Mr. Bellotti follow:]

PREPARED STATEMENT OF HON. FRANCIS X. BELLOTTI, ATTORNEY GENERAL, STATE OF MASSACHUSETTS

Mr. Chairman, members of the Subcommittee on Constitutional Rights, I thank you for this opportunity to speak to you on S. 2008 and related topics.

A little over a year ago, former Governor Francis W. Sargent of my state testified before this Subcommittee on an earlier draft of this same bill. I will not repeat his testimony, although I must begin with a shared conviction: The danger our democracy faces is not so much the specific outrages of future Watergates, but the continued and persistent encroachment by executive government agencies into the affairs of the states, and ultimately into the private lives of every one of us.

Nowhere is this threat to our democracy greater than in the area of federal criminal justice information systems, including the FBI's National Crime Information Center's computerized criminal history program and related manual identification files.

To realize how far we have come down this dangerous road, one has only to go back to the turn of the century when central registries of fingerprints were first established. At that time, fingerprints on persons found not guilty were returned to their subjects.

Today, the FBI's identification division has some 200 million fingerprints, including files on millions of individuals never even arrested for a crime.

Sixty years ago, when Congress first debated the establishment of the FBI, the single most expressed fear was that such a federal police force might someday

[1] See appendix, pp. 286–288.

adopt practices habitual to other countries. Congress was concerned that such an agency might someday engage in such practices as the "collection and lodgment in police files of rumors, suspicions, and gossip," as well as information about the private lives of persons who were not criminals.

Today, such information is computerized and disseminated around the country in microseconds.

Finally, one has only to look back two months, to May 20, and examine the new Justice Department regulations for criminal justice information systems to realize that this dangerous trend is accelerating.

Mr. Chairman, these regulations are unequivocable evidence of the Justice Department's unwillingness or inability to regulate itself and prevent further encroachment of 10th Amendment rights of the states and the basic constitutional rights of every citizen.

These regulations are a compelling testimony for the urgent need of legislation like that before us today. The regulations are totally inadequate. They do little more than codify existing inadequacies and lack of control over current federal criminal justice systems.

Worse, they help insure these systems become more intrusive and abusive.

The two major new problems raised by these regulations are:

1. By defining manual identification fingerprint-arrest rap sheets as part of the NCIC, these regulations permit the FBI to computerize existing manual files for inclusion into the NCIC/CCH over the specific objections of states, such as Massachusetts, Pennsylvania and New York, which have refused to participate in the NCIC/CCH. The result is to magnify the potential abuse of this system by a factor of 40 (from ½ million records to 20 million records).

2. These regulations pave the way for the FBI to control, to an extent previously unimagined, local police activities by controlling police telecommunications. The result again would be to run rough-shod over a presently state-controlled police system, The National Law Enforcement Telecommunications Systems, and replace it with a federally-controlled and monitored system.

Mr. Chairman, if the Massachusetts experience shows anything—and as you know we were one of the first states to legislate in this area—it is that to control these systems, to insure their effectiveness for law enforcement and privacy, self-regulation by administrative fiat does not work, nor will it ever work.

The basic mission of a police agency, whether it is the Boston Police or the FBI, is to investigate, maintain order, and arrest people.

Similarly the basic mission of the courts is to try cases; and the goal of prisons is to rehabilitate criminal offenders. However, none has as a primary goal—the collection, maintenance, dissemination and regulation of complete criminal history records.

Our experience shows that a separate agency must be established whose only mission is to regulate criminal justice information systems. Further, this agency should be established by law. This law should also lay down minimum standards to insure privacy and individual rights. (We must remember that privacy and law enforcement are not mutually exclusive. A major responsibility of the criminal justice system, after all, is to rehabilitate criminal offenders. This becomes impossible if past criminal records, promiscuously disseminated, prevent rehabilitation.)

In 1972, Massachusetts passed such a law, which established such an agency called the Criminal History System Board. I now serve as Chairman of this agency. Further, our legislation established basic standards to protect privacy.

Copies of this law have been made available to you so I won't describe it in detail. Generally, our law is in agreement with the standards set by S. 2008 with one important exception.

Under our law, access to criminal history records is limited to criminal justice agencies and agencies with specific statutory authority. Unlike S. 2008, access is not allowed by executive order. This is one of two major weaknesses in S. 2008.

For example, the Governor of our state cannot gain access to these files, except for consideration of a specific record of a person before him for a pardon.

Our insistence on statutory authority only has proven to be amply justified over the past two years.

Let me explain, with some recent history.

After Chapter 805 went into effect in 1972, Massachusetts was sued by the Justice Department in Federal District Court on behalf of the Small Business Administration, the Defense Investigatory Services, and 75 other federal agencies denied access under this provision.

Although these agencies did not have any congressional authorization for access, they all alleged that access was essential for a variety of reasons, including in the case of the defense investigatory services, "national security".

The case was finally dropped by then U.S. Attorney General Elliot Richardson. None of these agencies, to this day, receive those records they then alleged to need so desperately. But, as far as I know, all continue to operate effectively in the Commonwealth of Massachusetts. The Small Business Administration still gives out loans; Massachusetts citizens still are employed in defense-related projects.

The moral is clear. Many executive agencies may think they need access to these records, some with executive order approval, but most can get along without them. If they really need access, they should be willing to take their case to Congress.

There is another moral too. Although the Defense Investigatory Services alleged it needed these records for national security, it did not and does not get them, and top secret government research is still conducted at the Lincoln Lab at MIT. The national security has not been imperiled. If anything, recent disclosures concerning the Defense Investigatory Services, and its immediate predecessors, suggest that these agencies may have violated state and federal law by snooping into private lives of citizens. Perhaps they themselves were the real threat to the security of our democracy.

Mr. Chairman, my only other concern with S. 2008 is its failure to prohibit further federal intrusion into the area of local police telecommunications.

This is far too important an area to leave to an appointed commission for some time in the future. I think the President's Office of Telecommunications Policy has spoken authoritatively on this matter.

I quote from a letter from Acting Director John Edgar to former Attorney General William Saxbe written October 11, 1974:

"A growing federal role in (police telecommunications) would not only weaken the ability of the other levels of government to manage their own affairs, but also raises concerns about the protection of individual rights. . . . As we stated to you when we were first appraised of the FBI proposal, we fear that it could result in the absorption of state and local systems into a potentially abusive, centralized, federally-controlled communications and computer information system."

Mr. Chairman, with these two exceptions, I believe S. 2008 to be excellent, timely, and crucially important legislation. Passage will help us replace the current highly centralized, but loosely controlled, federal system, with a highly decentralized, strongly controlled, local and state-oriented system.

The present system remains intolerable. For this reason I am in the process of preparing, with other State Attorneys General, a suit to enjoin continued operations of the NCIC/CCH which violate constitutional rights and guarantees.

In response to an initial letter sent to all State Attorneys General, 15 shared this concern and only 6 disagreed, among those who responded.

I will leave with you copies of our law, Chapter 805, and current regulations pursuant to that act. I will also leave copies of our critique of the recent Justice Department regulations governing criminal justice information systems detailing their constitutional and statutory deficiencies.

I would be happy to answer any questions you might have.

Thank you.

THE COMMONWEALTH OF MASSACHUSETTS,
OFFICE OF THE SECRETARY,
*Boston, Mass., December 10, 1974.*

*Rules and Regulations filed in this Office under the provisions of chapter 30A as amended.*

Filed by: Criminal History Systems Board (R&R Approved by the Criminal History Board Pursuant to M.G.L. Chapter 6, Section 168 and 171)
Date filed: December 10, 1974
Date published: December 27, 1974
Chapter 233, sec. 75

Printed copies of rules and regulations purporting to be issued by authority of any department, commission, board or Officer of the Commonwealth or any city or town having authority to adopt them, or printed copies of any ordinances or town by-laws, shall be admitted without certification or attestations, but if this genuineness is questioned, the court may require such certifications or attestations thereof as it deems necessary.

Attested as a true copy.

JOHN F. X. DAVOREN,
*Secretary of the Commonwealth.*

THE COMMONWEALTH OF MASSACHUSETTS,
CRIMINAL HISTORY SYSTEMS BOARD,
*Boston, Mass., December 11, 1974.*

Attention: Mr. Sam Ebb
OFFICE OF THE SECRETARY OF THE COMMONWEALTH
*State House,*
*Boston, Mass.*

DEAR MR. EBB: Please make 10,000 copies of the regulations submitted to your office on behalf of the Criminal History Systems Board on December 10, 1974. It is my understanding that each copy of the regulations will cost approximately twenty-five cents ($.25), and that the total cost to the Board will amount to twenty-five hundred dollars ($2500). It is our expectation that this job should take approximately 10 days to two weeks. Please keep us informed of any changes.

Sincerely,

H. M. SHAFRAN,
*Assistant to the Chairman.*

---

THE COMMONWEALTH OF MASSACHUSETTS,
CRIMINAL HISTORY SYSTEMS BOARD,
*Boston, December 9, 1974.*

Hon. JOHN F. X. DAVOREN,
*Secretary of State,*
*State House, Boston, Mass.*

DEAR SECRETARY DAVOREN: Chapter 805 of the 1972 Massachusetts Statutes amended M.G.L. c.6 by adding sections 167 through 178. M.G.L. c.6 sec. 168 established the Criminal History Systems Board which has a duty to promulgate regulations regarding the collection, storage, dissemination and usage of criminal offender record information for purposes of protecting the security and privacy of such data under M.G.L. c.6, secs. 168 and 171.

The Criminal History System Advisory Committee submitted the first official draft of the regulations, and after due notice to your office and publication of legal notices in appropriate newspapers of general circulation public hearings were held on March 29, 1974 in Boston, April 24, 1974 in Fall River, and April 25, 1974 in Springfield. After these public hearings and with the benefit of comments therefrom, the Criminal History Systems Board met, discussed, modified, and acted upon these regulations in the course of twelve public meetings from May 10 through October 8, 1974. The result of this series of public meetings was an approved draft of the regulations. A second set of public hearings on the approved draft of the regulations was then held after due notice to your office and publication of legal notices in appropriate newspapers of general circulation on November 13, 1974 in Boston, November 14, 1974 in Fall River, and November 15, 1974 in Springfield. Subsequently, the Criminal History Systems Board held a public meeting on December 3, 1974, and after duly considering and acting upon suggestions received from the second set of hearings, revised the approved draft of the regulations and adopted the final version by a majority vote in excess of two thirds. An attested copy of these adopted regulations is attached hereto.

The Criminal History Systems Board is now submitting these regulations for publication in accordance with M.G.L. c.30, sec. 37 as amended.

Sincerely,

ARNOLD R. ROSENFELD,
*Chairman, Criminal History Systems Board.*

---

REGULATIONS APPROVED BY THE CRIMINAL HISTORY SYSTEMS BOARD PURSUANT TO M.G.L. CHAPTER 6 SECTIONS 168 AND 171 ON DECEMBER 3, 1974

*1.1 Records and data included in CORI*

*(a)* "Criminal offender record information" (CORI) means records and data compiled by criminal justice agencies for the purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation and release. Such information shall be restricted to that recorded as the result of the initiation of criminal proceedings or of any consequent proceedings related thereto. It shall not include intelligence, analytical and investigative reports and files, nor statistical records and reports in which individuals are not identified and from which their identities are not ascertainable.

(*b*) CORI is limited to records and data in abstract or line entry form which set forth the fact and results of an individual's movement through any one or more of the formal stages of the criminal justice process from the initiation of criminal proceedings through pretrial proceedings, prosecution, adjudication, correctional treatment, release and any consequent or related criminal justice proceedings. CORI shall be limited to factual statements about the occurrence and outcome of an arrest, indictment, warrant, arraignment, bail, continuance, default, trial, appeal, disposition, sentence, probation, commitment, parole, commutation, release, termination or revocation of probation or parole, pardon or similar occurrences and outcomes.

*1.2 Applicability of regulations*

These regulations shall control the content, access to, and dissemination of CORI in automated systems. These regulations shall control only the access to and dissemination of CORI in manual systems, but shall control the content of such manual systems with regard to any action taken under Regulations 3.9 and 3.10.

*1.3 Public records data*

CORI shall not include public records and data subject to disclosure under public record statutes, orders, or regulations if such records and data are limited to information concerning a single criminal justice proceeding within one criminal justice agency and contain no CORI relating to any other criminal justice agency.

*1.4 Statistical records and reports*

CORI shall not include statistical records and reports in which individuals are not identified and from which their identities are not ascertainable.

*1.5 Exclusion of juvenile data*

CORI shall include information concerning a person who is under the age of seventeen years if and only if that person is both adjudicated and receives a disposition as an adult.

*1.6 Inclusion of photographs and fingerprints*

In addition to other records and data, CORI shall include fingerprints, photographs, and similar identifying information and documents recorded as the result of the initiation of a criminal proceeding or any consequent proceedings provided, however, that CORI shall not include photographs of an individual used for investigative purposes if the individual is not identified by name.

*1.7 Initiation of criminal proceedings*

CORI shall be restricted to that information recorded as a result of the initiation of criminal proceedings or any consequent proceedings. "Initiation of criminal proceedings" means issuance of an arrest warrant, the arrest of an individual, issuance of a summons, indictment by a grand jury or issuance of a court complaint.

*1.8 Exclusion of intelligence, investigative and analytical reports, files and data*

(*a*) CORI shall not include intelligence, analytical and investigative reports or files such as police or prosecution initiated surveillance reports, informant reports, field interview information, field interrogation and observation reports and similar reports and files.

(*b*) CORI shall not include wanted posters and public announcements, photographs and other identifying data, concerning escapees or other wanted persons.

*1.9 Content of converted files*

No CORI concerning juveniles, juvenile offenses or acts of delinquency, minor motor vehicle offenses, or acts which are no longer criminal offenses, shall be converted from manual to computerized form for inclusion in the automated criminal offender record information system provided, however, that information relating to proceedings in which a juvenile both is adjudicated and receives a disposition as an adult shall be so converted. "Minor motor vehicle offenses" means those offenses not punishable by incarceration.

*1.10 Triggering of file conversion*

(*a*) Except as otherwise provided in these regulations, no CORI respecting any individual shall be converted from manual to computerized form for inclusion in the automated criminal offender record information system unless:

(i) such individual is presented in court and the Office of the Commissioner of Probation receives a current daily court slip concerning presentation in court on any charges other than a minor motor vehicle offense;

(ii) such individual has attained at least the age of seventeen years;
(iii) such individual has a prior conviction for a non-juvenile offense; and
(iv) there is either: (A) on file in the Department of Public Safety with respect to such individual a fingerprint card relating to a criminal arrest; or (B) a sufficient match by name, date of birth, father and mother's last name, address and social security or other identifying number to ensure that the accused person and the person about whom the file is maintained are the same person, and there is full compliance with Regulation 1.13.

(*b*) If an individual to whom CORI refers, including a juvenile who is both adjudicated and receives a disposition as an adult, is convicted of a felony as the result of a current court appearance, then CORI concerning such individual shall be converted if such individual meets all of the conversion criteria except those in Regulations 1.10 (a) (ii) and 1.10 (a) (iii) above concerning age and prior conviction for a non-juvenile offense.

*1.11 Conversion and removal of arrest entries without court activity data*

(*a*) CORI pertaining to an arrest which resulted in a non-guilty disposition as set forth in Regulation 1.14 shall not be converted from manual to computerized form pursuant to the Criminal History Record Conversion Project for inclusion in the automated CORI system.

(*b*) CORI pertaining to an arrest which resulted in a non-guilty disposition as set forth in Regulation 1.14 shall be removed from the automated CORI system.

*1.12 Inclusion of appellate court proceeding data*

CORI relating to appellate court proceedings shall be entered and maintained on the automated CORI system except as provided otherwise in these regulations.

*1.13 Requirement of stringent identification standards*

The director of teleprocessing shall, with the approval of the Criminal History Systems Board (CHSB) adopt procedures which will ensure there is sufficient data established for identification to produce a high degree of certainty that CORI maintained in the automated system is that of a specific individual.

*1.14 Nonguilty dispositions*

Nonguilty dispositions shall include any criminal proceeding in which the defendant has been found not guilty by the court or jury, or a no bill has been returned by the grand jury, or a finding of no probable cause has been made by the court, or a conviction has been reversed on appeal, or an arrest has not been followed by subsequent court activity within seven days unless the director of teleprocessing is informed by the appropriate law enforcement agency that such court activity has been prevented for medical reasons or escape of the individual.

*1.15 Restriction of certain records*

All CORI with respect to any criminal proceedings in which a nolle prosequi or dismissal has been entered, or the court has ordered the sealing of the records of such proceeding, shall be included in the automated CORI system provided, however, that such CORI shall not be maintained for on-line computer access nor shall it be disseminated from such system to any individual or agency except as provided in Regulation 1.18 (a), (b), (c), (f), or (g). With respect to CORI restricted in accordance with this regulation, the CHSB shall respond "no record" to inquiries from all agencies and individuals.

*1.16 Removal of certain CORI from the automated CORI system*

Except as provided in these regulations, all CORI with respect to active and/or pending criminal proceedings shall be included in automated CORI systems. CORI with respect to any criminal proceeding for which the individual receives a nonguilty disposition as defined in Regulation 1.14 shall be removed from the automated CORI system.

*1.17 Restriction of CORI regarding inactive felons and misdemeanants*

(*a*) CORI relating to an offense which would in this state be deemed a felony shall be removed from on-line storage and access and placed in an off-line mode in the automated CORI system, if (i) a period of seven years has elapsed from the date of court appearances and dispositions relating to the particular offense, including termination of court supervision, probation, parole, sentence or incarceration and (ii) the individual convicted of the particular offense has not been convicted of any criminal offense for the preceding seven year period except minor motor vehicle offenses.

(*b*) CORI relating to an offense which would in this state be deemed a misdemeanor and where the individual convicted of this particular offense has never

been convicted of an offense which would in this state be deemed a felony, except a felony directed to be placed off-line by paragraph (a) above, shall be removed from on-line storage and access and placed in an off-line mode in the automated CORI system, if (i) a period of five years has elapsed from the date of court appearance and dispositions relating to the particular offense, including termination of court supervision, probation, parole, sentence or incarceration; and (ii) the individual convicted of the particular offense has not been convicted of any criminal offense for the preceding five year period except minor motor vehicle offenses.

(c) With regard to parts (a) and (b) of this regulation no record shall be removed as to any individual against whom any criminal proceeding has been initiated and is currently pending.

(d) CORI referred to in parts (a) and (b) of this regulation shall not be maintained for on-line computer access nor shall it be disseminated from such system to any individual or agency except as provided in Regulations 1.18 and 1.19.

(e) The CHSB shall inform criminal justice agencies seeking such CORI that the information is "off-line". It shall respond "no record" to inquiries from non-criminal justice agencies.

*1.18 Restrictions on CORI removed from on-line access and dissemination*

CORI removed from on-line access and dissemination under Regulations 1.15 and 1.17 shall be held in confidence and shall not be made available for review by, or dissemination to, any individual or agency except as follows:

(a) Where necessary for internal administrative purposes of the CHSB or for the regulatory responsibilities of the CHSB, Criminal History System Advisory Committee, or Security and Privacy Council.

(b) Subject to the approval of the CHSB when the information is to be used for statistical compilations in which the individual's identity is not disclosed and from which it is not ascertainable or for purposes of research conducted in accordance with CHSB regulations.

(c) When the individual to whom the information related seeks to exercise rights of access and review under the provisions of Regulations 3.9 and 3.10 or the information is necessary to permit adjudication under the provisions of Regulations 3.9 and 3.10 of any claim by the individual to whom the information relates that it is misleading, inaccurate or incomplete.

(d) When a criminal justice agency is required pursuant to a statute to utilize such information for pre-employment investigations of its prospective employees; *Provided, however,* That in such case the criminal justice agency shall receive only such information as is required by statute to discharge its responsibilities.

(e) When CORI restricted under the provisions of Regulation 1.17 is required for impeachment of a witness in any judicial proceeding and a valid court order is received ordering release of such CORI for such purpose.

(f) When there has been a finding or verdict of guilt on an offense punishable by more than six months incarceration, CORI removed from on-line access and storage shall be made available to the probation officer and judge for sentencing purposes only.

(g) When the chief executive officer of a criminal justice agency certifies that such information is necessary for the conduct of a pending criminal investigation.

*1.19 Listing of all CORI removed from on-line access and dissemination*

The director of teleprocessing shall maintain a listing of all CORI removed from on-line access and dissemination under the provisions of Regulations 1.15 and 1.17. This listing shall be used only to effectuate the provisions of Regulations 1.15, 1.17 and 1.18.

*1.20 Restoration of CORI to on-line access and dissemination*

CORI removed from on-line access and dissemination under provisions of Regulation 1.17 shall be restored to on-line access and dissemination only to criminal justice agencies in the automated CORI system if the individual to whom such CORI relates has been found guilty of a subsequent offense punishable by incarceration for not less than six months.

*1.21 Court or administrative orders sealing or purging CORI*

(a) Upon any valid, final court or administrative order requiring sealing of any CORI, the CHSB shall restrict the access and dissemination of such CORI in accordance with the provisions of Regulation 1.18 and the tenor of such order.

(b) Upon any valid, final court or administrative order, requiring the purging of any CORI, the CHSB shall remove such CORI from the automated CORI system so that there is no trace of the information and no indication that it was removed.

*1.22 Notification of closing or removal of CORI*

(*a*) In the event that any CORI is removed from the automated CORI system in accordance with these regulations, all agencies or individuals to whom such CORI has been disseminated shall be promptly notified of the removal of such CORI.

(*b*) The CHSB shall provide those agencies notified under 1.22 (a) with appropriate instructions as to what action should be taken in accord with these regulations.

*2.1 Definition of criminal justice agencies*

Criminal justice agencies means those agencies at all levels of government which perform as their principal function activities relating to (a) crime prevention, including research or the sponsorship of research, (b) the apprehension, prosecution, adjudication, incarceration or rehabilitation of criminal offenders, or (c) the collection, storage, dissemination or usage of criminal offender record information.

*2.2 Governmental units qualifying as "criminal justice agencies"*

(*a*) For the purpose of M.G.L. c.6 secs. 167–178, and these regulations, the phrase "criminal justice agencies" shall include an office, department, board, commission, municipal corporation and the like, created by statute or constitution and any subunit thereof, created by statute or constitution, which performs as its principal function activities set forth in M.G.L. c.6 sec. 167.

(*b*) In the case of a statutorily or constitutionally created non-criminal justice office, department, board, commission, municipal corporation or the like, the phrase "criminal justice agencies" shall include any administratively created subunits which perform as their principal function, activities set forth in M.G.L. c.6 sec. 167 and which demonstrate to the CHSB a substantial need to have access to CORI.

*2.3 Definition of "at all levels of government"*

Agencies at all levels of government shall be restricted to agencies of the state, local, county or federal governments including intrastate and interstate regional bodies established by state or federal constitutions or by the legislative or executive branches of government and which are supported by public funds. The term "agencies" shall include comparable units of foreign governments.

*2.4 Definition of "principal function"*

In order to qualify as a criminal justice agency, an agency must perform as its principal function, activities set forth in M.G.L. c.6 sec. 167. Agencies seeking access to criminal offender record information shall demonstrate to the satisfaction of the CHSB that they have the requisite statutory authority and do, in fact, perform such activities by proof that they allocate a substantial portion of their time, money, personnel and other resources to such activities.

*2.5 Definition of "crime prevention"*

Crime prevention shall mean activities performed by police and prosecutorial agencies to deter criminal conduct.

*2.6 Definition of "apprehension"*

Apprehension means activities including but not limited to arrest of adults by police or other criminal justice agencies and setting of conditions of pre-trial release by bail commissioners and masters in chancery.

*2.7 Definition of "prosecution"*

Prosecution means activities relating to issuance of complaints and arrest warrants, indictments, preparation for and conducting of criminal trials and any subsequent proceedings related to such trials performed by grand juries, the Department of the Attorney General, district attorneys or other prosecutors.

*2.8 Definition of "adjudication"*

Adjudication means those activities including but not limited to conduct of criminal trials, the making of findings, and disposition of adults in courts of criminal jurisdiction and the activities of court clinics and the Division of Legal Medicine of the Department of Mental Health in competency and related matters relating to adult criminal proceedings.

*2.9 Definition of "incarceration"*

Incarceration means activities including but not limited to pretrial and post-conviction detention of adults in police lock-ups, jails, houses of correction, and

adult correctional institutions and the detention of adults in mental health institutions in cases involving drug violations, transfers from correctional institutions, criminal competency determinations, and acquittal by reason of insanity.

*2.10 Definition of "rehabilitation"*

Rehabilitation means activities performed by courts, probation offices, correctional institutions and parole agencies, among others, intended for the treatment, care, supervision or social readjustment of adults who have been adjudicated guilty, sentenced or against whom criminal charges are pending.

*2.11 Definition of activities relating to "the collection, storage, dissemination or usage of CORI"*

Activities relating to the collection, storage, dissemination or usage of CORI means those activities performed by the CHSB, Criminal History System Advisory Committee (CHSAC), the Security and Privacy Council and those performed by agencies at all levels of government operating criminal justice information systems.

*2.12 Juvenile agencies which perform criminal justice functions*

Agencies of the juvenile justice system which perform as their principal function criminal justice activities with respect to juveniles shall be deemed criminal justice agencies for the purposes of receiving CORI from CORI systems, M.G.L. c.6 secs. 167–178, and these regulations.

*2.13 Persons within criminal justice agencies eligible for access to CORI*

(*a*) CORI shall be disseminated under the provisions of M.G.L. c.6 sec. 172(a) only to those officials and employees of criminal justice agencies determined by the administrative heads of such agencies to require such information for the actual performance of their criminal justice duties. Such administrative heads shall maintain and keep available for inspection by the CHSB a list of such authorized employees by position, title or name.

(*b*) Consultants and contractors to criminal justice agencies shall have access to CORI only if such access is specified in their contract and is essential to performance or contractual obligations related to the management or computerization of CORI. In addition, no criminal justice agency shall disseminate CORI to or permit access to CORI by any consultant or contractor unless it has obtained the prior written approval of the CHSB for such dissemination or access.

(*c*) Consultants and contractors to criminal justice agencies having access to CORI shall complete a written agreement to use CORI only as permitted by M.G.L. c.6 secs. 167–178 and these regulations with such agreement to be held by the criminal justice agency and subject to review by the CHSB.

*2.14 Limitations on access*

Criminal justice agencies shall request and have access only to such CORI as is reasonably necessary for the actual performance of such agencies' criminal justice duties and responsibilities.

*2.15 Dissemination outside a certified subunit of a non-criminal justice agency*

A certified criminal justice agency which is a subunit of a non-criminal justice agency shall disseminate CORI only in accordance with the provisions of Regulation 2.13. In no case shall CORI be disseminated from the subunit, directly or through any intermediary, to any unauthorized official, employee, contractor or consultant of the non-criminal justice agency of which it is a part.

*2.16 Definition of individuals and agencies authorized access by sec. 172(b)*

(*a*) Except as provided in M.G.L. c.6 secs. 167–178 and these regulations, criminal offender record information shall be disseminated only to such noncriminal justice individuals and agencies as are authorized access to such information by statute.

(*b*) "Authorized access by statute" means that there be a specific statutory directive that such individual or agency have access to CORI or a statutory requirement that such individual or agency consider CORI in his or its decision-making process.

(*c*) Such directive or requirement imposed solely by administrative or executive rule or regulation shall not constitute sufficient authorization for access to CORI.

(*d*) A statutory requirement that an individual or agency consider "good character", "moral character", "trustworthiness" and the like, in its decision-making process shall not constitute sufficient authorization for access to CORI.

*2.17 Limitations on dissemination of CORI*

To the extent practicable, only such CORI as is necessary for the discharge of the statutory responsibilities of an individual or agency authorized access under M.G.L. c.6 sec. 172(b) shall be requested and disseminated to such individual or agency. If such responsibilities can be discharged by answers to specific questions, then, to the extent practicable, only such CORI shall be requested and disseminated as is necessary to answer such questions.

*2.18 Use of CORI for rehabilitation purposes*

(*a*) Officials and employees of criminal justice agencies engaged in rehabilitative activities may allow consultants directly under their supervision and control who are also associated with educational institutions, half-way houses, group residences, social service agencies, medical practitioners or similar individuals to utilize, but not disseminate, CORI for purposes of obtaining services or benefits for individuals named in such CORI for whom they are responsible, provided that each of such individuals involved, himself, gives his informed consent to such access.

(*b*) Consultants utilizing CORI under the provisions of Regulation 2.18(a) shall:

(i) establish their status as full-time or part-time employees of such criminal justice agency(ies), or as individuals who have contracts with such criminal justice agency(ies) by documentation submitted to the CHSB;

(ii) be subject to the provisions of Regulations 2.13–2.15;

(iii) use CORI only under the direct supervision and control of such criminal justice agency officials and/or employees;

(iv) be notified that the retention and dissemination of such CORI is subject to the provisions of M.G.L. c.6 secs. 167–178 and these regulations;

(v) not disseminate such CORI to any agency or individual outside of the criminal justice agency having custody of the CORI, except that reports based on, but not containing the CORI, which recommended rejection or admission to a program, or prescribe treatments, services, and/or benefits for the individual, may be conveyed to the rehabilitative agency or individual with whom such consultant is associated; and

(iv) complete a written agreement not to disclose any CORI and to use CORI only as permitted by this regulation, with such agreement to be held by the criminal justice agency and subject to review by the CHSB.

*2.19 Access by out-of-state agencies*

(*a*) Except for purposes of approved research under M.G.L. c.6 sec. 173, CORI shall be disseminated only to federal, state and local agencies in other countries and states which are eligible for access to CORI under the provisions of M.G.L. c.6 secs. 172(a) and 172(b).

(*b*) The CHSB shall maintain a list of federal, state and local agencies qualifying under the provisions of M.G.L. c.6 secs. 172(a) and 172(b), and these Regulations.

(*c*) Unless a blanket statement concerning restrictions on access and dissemination of CORI has previously been sent, all CORI dissemination to eligible out-of-state and federal agencies shall be accompanied by a copy of M.G.L. c.6 secs. 167–178 and regulations adopted thereunder, a written statement of the requirements for compliance with such restrictions and sanctions for non-compliance.

(*d*) Any out-of-state or federal agencies which the director of teleprocessing has reason to believe have violated the provisions of M.G.L. c.6 secs. 167–178 or the regulations adopted thereunder may have their eligibility for access to CORI suspended for a period of ten days by the director of teleprocessing pending further consideration and action by the CHSB.

*2. 20 Computer terminal access to CORI by noncriminal justice agencies*

Authorized noncriminal justice agencies or individuals and criminal justice subunits of such agencies and out-of-state agencies shall not have direct computer terminal access to CORI. Such access shall be effected only through central control terminals designated for such purpose by the CHSB.

*2. 21 Access by other than personal identifying information*

Except for approved research programs, access and dissemination of CORI shall be limited to inquiries based on name, fingerprints, or other personal identifying characteristics. No CORI shall be disseminated to authorized criminal justice agencies whose inquiries are based upon categories of offenses or any data elements other than personal identifying characteristics unless such individuals

or agencies have first obtained written authorization from the Commissioner of Probation or his deputy for access based on other than personal identifying characteristics which would identify a specific individual.

*2. 22 Definition of "dissemination"*

Dissemination means the release, transfer or divulgence of CORI in any manner or form including permitting any person to inspect and/or copy CORI.

*2. 23 Definition of "automated CORI system"*

Automated CORI system means the data processing and communications system operated and maintained by the CHSB in accordance with the provisions of M.G.L. c.6 sec. 168 for the collection, storage, exchange, dissemination and distribution of CORI.

*2. 24 Certification procedures*

(*a*) Any individual or agency requesting certification for access to CORI under the provisions of M.G.L. c.6 sec. 172 shall apply in writing to the CHSB.

(*b*) The application shall be on a form provided by the CHSB and shall contain the name and address of the applicant, the subsection of M.G.L. c.6 sec. 172 under which it seeks access, and a statement of the basis upon which such access is sought. The applicant shall include with his application documentary evidence which establishes its eligibility for access to CORI under M.G.L. c.6 sec. 172 and these regulations. A copy of the application and accompanying materials shall be sent by the applicant to the Security and Privacy Council.

(*c*) The CHSB may require the applicant to submit such additional evidence of eligibility and to make such presentations to the CHSB as the CHSB deems necessary.

(*d*) If an application for certification is received at least 21 days prior to the next regularly scheduled meeting of the CHSB, the CHSB shall consider it at such meeting. Applications received less than 21 days prior to regularly scheduled CHSB meetings shall be considered at the next subsequent meeting of the CHSB.

(*e*) The CHSB shall make a finding in writing of the eligibility or non-eligibility of an applicant for access to CORI. Such written finding, together with a written statement of the reasons for the CHSB's decision shall be sent to the applicant forthwith.

*3.1 Notice to individuals of the existence of CORI concerning them*

The Board shall give notice to each individual in the following manner as to the existence of CORI concerning him:

(*a*) When a criminal defendant first comes to court in connection with his case, the probation officer shall give him in hand a notice, on a form approved by the director of teleprocessing, advising the defendant in clearly understandable language of the existence of CORI, of his rights of inspection, protest and removal of CORI relating to him from on-line access under these regulations and that he may have, on request, a copy of these regulations. If requested, the probation officer shall give him a copy of these regulations.

(*b*) When a present or former criminal defendant is discharged by a court, released from probation or from incarceration under sentence without parole or is otherwise separated or about to be separated from the criminal justice system, if not at substantially the same time as in paragraph (a), above, the probation, parole or other officer or person dealing with him shall give him in hand the notice set forth in paragraph (a), above, and if requested, a copy of these regulations.

(*c*) When the automated CORI system commences on-line operations, or reasonably soon thereafter, the director of teleprocessing shall cause to be sent by first class mail to each individual on whom CORI is held in such system a notice substantially as set forth in paragraph (a), above; and if, thereafter, any such individual requests a copy of these regulations, the director shall cause the same to be mailed to said individual.

(*d*) Within 90 days after the CORI system commences on-line operations, and annually thereafter, the director of teleprocessing shall file with the Secretary of State and cause to be published in one or more newspapers of general circulation in each standard metropolitan statistical area of the Commonwealth, as defined by the United States Bureau of the Census, once each week for three consecutive weeks a notice setting forth in clearly understandable language the following:

(1) the name of the CORI system and the title and address of the director of teleprocessing;

(2) the purpose of the CORI system;

(3) the definition of CORI or a paraphrase thereof in clearly understandable language;

(4) the approximate number of individuals about whom information is then held in the CORI system;

(5) that the CORI is held in computerized form;

(6) a generalized description of the persons and organizations having access to the system;

(7) notification that any individual who thinks CORI with respect to him is held in the system may have a search made, and, if such information is so held, may inspect, copy and object to it as provided in these regulations; and

(8) a statement that the notice is published in compliance with these regulations and an indication as to where a copy of these regulations may be obtained.

The director of teleprocessing shall see that copies of these regulations are deposited and freely available to the public, on request, at all of the places where CORI may be inspected under Regulation 3.5.

*3.2 Inspection of CORI in manual information systems*

Agencies at which criminal offender records are sought to be inspected shall prescribe reasonable hours and places of inspection, and shall impose such additional restrictions as may be approved by the CHSB, including fingerprinting, as are reasonably necessary both to ensure the record's security and to verify the identities of those who seek to inspect them.

*3.3 Release of data to individual*

(*a*) Each individual shall have the right to inspect or copy CORI relating to him in accordance with M.G.L. c.6 sec. 175 and these regulations.

(*b*) Any individual who is denied the right to inspect or copy CORI relating to him may, within 30 days of such denial, petition the CHSB for an order requiring the release of such CORI to him, with a copy of such petition to be sent to the Security and Privacy Council. The CHSB shall act on such petition within a reasonable time.

*3.4. Copying of records*

An individual shall, if practicable, be permitted to receive a computer printout or photocopy of CORI referring to him. The reviewing individual may make a written summary or notes in his own handwriting of the information reviewed, and may take with him such summary or notes. Before releasing any exact reproduction or hard copy of CORI to an individual, the agency holding the same shall remove all personal identifying information from the CORI. Such agency may, with prior approval of the CHSB, impose a reasonable charge for copying services. The director of teleprocessing shall provide forms for seeking access to CORI.

*3.5 Inspection of CORI in the automated CORI system*

CORI maintained in the automated CORI system shall be available for inspection by the individual to whom it refers only at reasonably convenient locations designated by the CHSB. The CHSB shall designate at least one such location within each county.

*3.6 Parties authorized to inspect and copy CORI*

An individual to whom CORI refers, or his attorney, or legal representative who is a law student, or any authorized agent of his attorney who is also an attorney holding a sworn written authorization from such individual and able satisfactorily to identify himself shall be permitted to inspect and copy such CORI for such individual's personal use in accordance with the requirements of 3.4.

*3.7 Review of a record and verification or exceptions*

(*a*) Each individual reviewing CORI shall be informed by the holding agency of his rights of challenge under M.G.L. c.6 sec. 175. Each such individual shall be informed that he may submit written exceptions to the agency concerning the information's contents, completeness, accuracy, mode of maintenance and/or dissemination.

(*b*) A record of each review shall be maintained by the holding agency on a form provided or approved by the CHSB. Each such form shall be completed and signed by the supervisory employee or agent present at the review and the reviewing individual. The form shall include a recording of the name of the reviewing individual, the date of the review, and whether or not any exception was

taken to the accuracy, completeness, contents, mode of maintenance and/or dissemination of the information reviewed. The record of each review which is kept to meet requirements of this section shall be open only to the CHSB, the Security and Privacy Council, and the individual.

*3.8 Recording of and action upon exceptions*

(*a*) Should an individual elect to submit exceptions to the contents, accuracy, completeness, mode of maintenance and/or dissemination of the CORI referring to him, he shall record such exceptions on a form provided or approved by the CHSB. The form shall include an oath or affirmation signed by the individual, that the exceptions are made in good faith and that they are to the best of the individual's knowledge and belief true. One copy of the form shall be forwarded to the review officer or officers of the criminal justice agency in question. An officer or officers shall be designated for that purpose in each criminal justice agency and their names submitted to the CHSB. A second copy of the form shall be forwarded to the CHSB.

(*b*) The criminal justice agency shall, within thirty days of the filing of written exceptions, complete an audit of the individual's criminal offender record information appropriate to determine the accuracy of the exceptions. The CHSB, the individual and the contributing agency shall be informed in writing of the results of the audit and be provided with copies of source documentation relevant to disputed CORI. Should the audit disclose inaccuracies or omissions in the information, the criminal justice agency shall within ten days of the completion of the audit cause appropriate alterations or additions to be made and notice of its actions to be given to the CHSB and the individual involved. Any other agencies in this or any other jurisdiction to which the criminal offender record information had previously been disseminated shall be notified by the criminal justice agency holding the record to alter their records accordingly.

(*c*) A copy of the form on which the exceptions have been recorded, written audit results, copies of source documents and the agency's written decision on any exceptions shall be forwarded to the Security and Privacy Council.

(*d*) Such records as are kept to meet the requirements of this section shall be available only to the CHSB, the Security and Privacy Council, the criminal justice agency and the individual.

*3.9 Challenges to the accuracy or completeness of criminal offender record information*

Any person who believes that criminal offender record information which refers to him is inaccurate, incomplete, or improperly maintained or disseminated may request any criminal justice agency in this State with custody or control of the information to purge, modify or supplement that information. Should the agency decline to purge, modify or supplement such CORI, or should the individual believe the agency's decision to be otherwise unsatisfactory, the individual may request review by the Security and Privacy Council within thirty (30) days of the agency's decision. Failure of the agency to act within the time prescribed in Regulation 3.8 shall be deemed a decision adverse to the complainant.

*3.10 Review by the CHSB of the Council's recommendations*

(*a*) The Security and Privacy Council shall issue written findings to the CHSB within 60 days of the receipt of the request for review. The CHSB shall within ten days of the receipt of any recommendations of the Council make its findings and disseminate its orders, if any, to individuals and agencies to which the records in question have been communicated as well as to the individual to whom the CORI refers.

(*b*) The CHSB may require the individual challenging the record and any criminal justice agency within the State to file or present in person such written and oral statements, testimony, documents and arguments as the interests of justice may require.

(*c*) The CHSB shall issue written findings of fact, conclusions and orders, in which the relief to which an individual is entitled and the basis of its decision are fully and specifically described. Findings, conclusions and orders shall be adopted by a majority vote of the CHSB.

*3.11 Burden of proof*

The individual challenging the validity of CORI shall have the burden in any proceedings before the CHSB of establishing reasonable grounds for believing that such CORI is inaccurate, incomplete, misleading or improperly maintained or disseminated. If such reasonable grounds are established in accordance with these regulations, the criminal justice agency holding the challenged CORI shall

have the burden of proving by a preponderance of the evidence that the exceptions to the record are not well taken and that the CORI should not be deleted, modified or supplemented in whole or in part, or any order issued.

*3.12 Circulation of challenged records*

CORI challenged under the provisions of these regulations shall be deemed to be accurate, complete and valid until otherwise ordered by the CHSB. Challenged CORI may be disseminated to authorized individuals and agencies but only with a notation stating that the validity of such CORI is being challenged and the basis for such challenge. Agencies disseminating such CORI shall maintain complete and accurate records of agencies and individuals to whom they disseminate such challenged CORI.

*3.13 Protection from accidental loss or injury*

The director of teleprocessing of the CHSB with the approval of the CHSB shall institute procedures for protection of information in the automated CORI system from environmental hazards including fire, flood and power failure. Appropriate elements shall include:

(*a*) adequate fore detection and quenching systems;
(*b*) watertight facilities;
(*c*) protection against water and smoke damage;
(*d*) liaison with local fire and public safety officials;
(*e*) fire resistant materials on walls and doors;
(*f*) emergency power sources; and
(*g*) back-up files.

*3.14 Protection against intentional harm*

(*a*) The director of teleprocessing with the approval of the CHSB shall adopt security procedures which limit access to information in the automated CORI system. These procedures shall include use of guards, keys, badges, passwords, access restrictions, sign-in logs, or like safeguards.

(*b*) All facilities which house the main automated CORI system shall be so designed and constructed as to reduce the possibility of physical damage to the information. Appropriate steps in this regard should include: physical limitations on access; security storage for information media; heavy duty, nonexposed walls; perimeter barriers; adequate lighting; detection and warning devices; and closed circuit television.

(*c*) The director of teleprocessing shall, with the approval of the CHSB, determine the number and location of, and the security requirements applicable to, remote computer terminals on the automated CORI system. The CHSB and the Security and Privacy Council shall have the right to enter the premises of any agency having such terminals for the purpose of inspecting such terminals and related facilities.

*3.15 Unauthorized access*

The director of teleprocessing shall, with the approval of the CHSB, maintain controls over access to information in the automated CORI system by requiring identification, authorization, and authentication of system users and their need and right to know. Appropriate processing restrictions and management techniques shall be employed to ensure information security in the automated CORI system. The CHSB shall be notified of any threats to the system.

*3.16 Personnel security*

(*a*) The director of teleprocessing and the heads of all agencies administering CORI systems shall cause to be investigated the previous employment and criminal record of employees and contractors assigned to CORI systems.

(*b*) Investigations shall be conducted prior to assignment to the CORI system. Willful giving of false information shall disqualify an applicant or employee from assignment to the CORI system.

(*c*) Each employee and contractor assigned to a CORI system shall be required to understand all rules and regulations applicable to such system. The director of teleprocessing shall establish appropriate programs of formal training concerning system security and privacy each year.

*3.17 Personnel clearances*

(*a*) All personnel assigned to the automated CORI system, including those having access to remote terminals, shall be assigned by the director of teleprocessing an appropriate security clearance which shall be renewed annually after investigation and review. The director of teleprocessing shall report periodically to the CHSB concerning issuance of personnel clearances.

(*b*) Personnel shall be granted security clearances for access only to such sensitive places, things and information as they have a demonstrated need and right to know.

(*c*) No person shall have access to any place, thing or information of a higher sensitivity classification than the highest valid clearance held by such person.

(*d*) Clearances shall be granted by the director of teleprocessing on a selective and individual basis following appropriate background investigations and review and strict adherence to need and right-to-know principles.

(*e*) Clearances shall be periodically reviewed to ensure that each employee is accorded the lowest possible clearance consistent with his responsibilities.

(*f*) Clearances shall be executory and may be revoked or reduced to a lower sensitivity classification at the will of the grantor. Adequate notice must be given of the reduction or revocation to all other agencies that previously relied upon such clearances.

(*g*) To provide evidence of a person's sensitivity classification clearance, the grantor of such clearance shall provide an authenticated card or certificate. Responsibility for control of the issuance, adjustment or revocation of such documents shall rest with the grantor. All such documents shall have an automatic expiration date requiring affirmative renewal annually.

*3.18 Implementation of security classification system*

The director of teleprocessing shall, with the approval of the CHSB, implement a sensitivity classification system for the automated CORI system including remote terminals. The general guidelines for this purpose are:

(*a*) Places and things shall be assigned the lowest classification consistent with their proper protection.

(*b*) Appropriate utilization of classified places and things by qualified users shall be encouraged.

(*c*) Whenever the sensitivity of places or things diminishes or increases, it shall be reclassified without delay.

(*d*) In the event that any place or thing previously classified is no longer sensitive and no longer requires special security or privacy protection, it shall be declassified.

*3.19 Classification guidelines*

Places and things included in the automated CORI system shall be classified by the director of teleprocessing with the approval of the CHSB in accordance with the following system:

(*a*) Secret—places and things which require maximum special security provisions and particularized privacy protection.

(*b*) Confidential—places and things which require a high degree of special security and privacy protection.

(*c*) Restricted—places and things which require minimum special security consistent with good security and privacy practices.

*3.20 System certification*

Before the automated CORI system commences on-line operations and periodically thereafter, the CHSB shall request and receive from an independent panel of three to five consultants a system certification attesting that the system as designed and operated is substantially secure against unauthorized access and otherwise performs substantially as is necessary to ensure compliance with these regulations.

*3.21 Listing of dissemination of CORI*

Each agency or individual authorized to disseminate CORI shall maintain a listing of both CORI disseminated and the agencies or individuals both within and outside the Commonwealth to which it has disseminated each item of CORI. Such listings shall be maintained in a form prescribed by the CHSB, for at least one year from the day of each such dissemination and indicate the agencies or individuals to whom such CORI was disseminated. Such listing shall be made available for audit or inspection by the CHSB, the CHSAC or Security and Privacy Council at such times as the CHSB, CHSAC or Council shall require.

*3.22 Administrative sanctions*

(a) Any employee of any criminal justice agency who violates the provisions of M.G.L. c. 6 secs. 167–178, these regulations, or security standards for automated CORI systems established under them, shall, in addition to or in lieu of any applicable criminal or civil penalties, be denied access to CORI by the CHSB and be administratively disciplined by suspension, discharge, reduction in grade, transfer or such other administrative penalties provided, however, that

such penalties shall be imposed only if they are permissible under any applicable statutes and/or contracts governing the terms of employment of the employee or officer in question.

(*b*) Any agency or individual authorized access to the automated CORI system who violates the provisions of M.G.L. c.6 secs. 167–178, these regulations or security standards established under them, may, in addition to any applicable civil or criminal penalties, be denied access to CORI in such system for such periods of time as the CHSB deems reasonable and appropriate.

*4.1 Definition of "Regulation"*

Regulation includes the whole or any part of any rule, regulation, standard or other requirement of general application and future effect, including the amendment or appeal thereof, adopted by the CHSB to implement or interpret the law enforced or administered by it, but does not include (a) an advisory ruling issued by it; (b) procedures concerning only the internal management or discipline of of the CHSB, and not substantially affecting the rights of or the procedures available to the public or that portion of the public affected by the CHSB's activities; or (c) decisions issued in adjudicatory proceedings.

*4.2 Petition for issuance, amendment, or repeal of regulation*

Any interested person or his attorney may file with the CHSB a petition for the adoption, amendment or repeal of any regulation. The petition shall be addressed to the CHSB and sent to the chairman by mail or delivered in person during normal business hours. All petitions shall be signed by the petitioner or his attorney, contain his address or the address of his attorney, set forth clearly and concisely the text of the proposed regulation, and shall include any data, facts, view or arguments deemed relevant by the petitioner, and shall be verified.

*4.3 Initial procedure to handle recommended regulations*

Upon receipt of a petition for the adoption, amendment or repeal of a regulation submitted pursuant to Regulation 4.1 or upon written recommendation by a member of the CHSB that a regulation be adopted, amended, or repealed, the CHSB shall determine whether to schedule the petition or recommendation for further proceedings in accordance with Regulation 4.4. If the regulation has been presented to the CHSB under Regulation 4.2, the chairman of the CHSB shall, within ten days after such determination, notify the petitioner of the CHSB's action.

*4.4 Procedure for the adoption, amendment, or repeal of regulations when a public hearing is required*

(*a*) Notice. Notice of a public hearing shall be given at least twenty-one (21) days prior to the date of the hearing unless some other time is specified by any applicable law. The CHSB shall notify the Secretary of State of the public hearing at least thirty (30) days in advance thereof in accordance with M.G.L. c.30A sec. 2. The CHSB shall publish the notice in at least one (1) newspaper of general circulation, and where appropriate, in such trade, industry or professional publications as the CHSB may select. The CHSB shall likewise notify in writing any person specified by any law and any person or group which has filed a written request for notice pursuant to Regulation 4.8.

The notice shall contain the following:

(i) the CHSB's statutory authority to adopt the proposed regulations;

(ii) the time and place of the public hearing;

(iii) the express terms or the substance of the proposed regulation; and

(iv) any additional matter required by any law.

The above notwithstanding, the CHSB shall also comply with any applicable statute which contains provisions for notice which differ from those contained herein.

(*b*) Procedure. On the date and at the time and place designated in the notice referred to in Regulation 4.4(a), the CHSB shall hold a public hearing. The meeting shall be opened, presided over and adjourned by the chairman or other member designated by the chairman. Within ten (10) days after the close of the public hearing, written statements and arguments may be filed with the CHSB unless the CHSB in its discretion finds such to be unnecessary. The CHSB shall consider all relevant matter presented to it before adopting, amending or repealing any regulation.

(*c*) Oral participation. Any interested person or his duly authorized representative, or both, shall be given an opportunity to present oral statements and arguments. In its discretion, the CHSB may limit the length of oral presentation.

(*d*) Emergency rule. If the CHSB finds that the immediate adoption of a regulation is necessary for the public health, safety or general welfare, and that observance of requirements of notice and public hearings would be contrary to the public interest, the CHSB may dispense with such requirements and adopt the regulation as an emergency regulation. The CHSB's finding and a brief statement of the reasons for its finding shall be incorporated in the emergency regulations as filed with the Secretary of State. Any emergency regulation so adopted shall state the date on which it is to be effective and the date upon which it shall expire. If no effective date is stated, the regulation shall be presumed to take effect upon being filed with the Secretary of State under Regulation 4.6. An emergency regulation shall not remain in effect for longer than three (3) months unless during the time it is in effect the CHSB gives notice and holds a public hearing and adopts it as a permanent regulation in accordance with these regulations.

*4.5 Availability of regulations*

The chairman of the CHSB shall be responsible for keeping a book containing all the CHSB's regulations. All the regulations of the CHSB shall be available for inspection during normal business hours at the CHSB's offices. Copies of all rules shall be available to any person on request. The CHSB may charge a reasonable fee for each copy.

*4.6 Filing of regulations*

Upon the adoption of a regulation, an attested copy shall be filed with the Secretary of State together with a citation of the statutory authority under which the regulation has been promulgated. The regulation shall take effect upon publication pursuant to M.G.L. c.30A sec. 6 unless a later date is required by any law or is specified by the CHSB.

*4.7 Advisory ruling*

Any interested person or his attorney may at any time request an advisory ruling with respect to the applicability to any person, property, or factual situation of any statute or regulation enforced or administered by the CHSB. The request shall be addressed to the CHSB and sent to the chairman of the CHSB by mail or delivered in person during normal business hours.

All requests shall be signed by the person making it or his attorney, contain his address or the address of his attorney, and state clearly and concisely the substance or nature of the request. The request may be accompanied by any supporting data, views or arguments. If the CHSB determines that an advisory ruling will not be rendered, the CHSB shall as soon as practicable notify the petitioner that the request is denied. If an advisory ruling is rendered, a copy of the ruling shall be sent to the person requesting it or his attorney.

The CHSB may notify any person that an advisory ruling has been requested and may receive and consider arguments, views, or data from persons other than the person requesting the ruling.

*4.8. Request for notice of hearings*

(*a*) Who may file. Any person or group may file a request in writing to receive notice of hearings or regulations which may affect such person or group.

(*b*) Form of request. The request shall contain the following:

(i) name of person or group;

(ii) address; and

(iii) subject matter of regulations which may affect the person or group

(*c*) When filed. The request shall be filed with the chairman of the CHSB and shall be renewed during the month of December to remain effective during the subsequent calendar year.

*4.9 Contents of regulations*

The CHSB will incorporate in any regulation adopted a concise general statement of their basis and purpose.

*4.10 Grant of hearing*

A public hearing will be granted whenever the CHSB seeks to revoke any certification granted under M.G.L. c.6 sec. 172 and otherwise as the CHSB may determine in specific cases. The CHSB may call informal public hearings, not required by statute, to be conducted under the regulations where applicable, for the purpose of rulemaking or to obtain information necessary or helpful in the determination of its policies, or the carrying out of its duties, and may request the attendance of witnesses and the production of evidence.

*4.11 Calendar*

The chairman of the CHSB shall maintain a docket and a hearing calendar of all proceedings set for hearing. So far as practicable, hearings shall be heard in the order in which they have been listed on the CHSB's docket.

*4.12 Place*

All hearings shall be held at Boston at the offices of the CHSB unless by statute or vote of the CHSB a different place is designated.

*4.13 Settlement: pre-hearing procedure*

(*a*) Opportunity for information settlement.

Where time, the nature of the proceeding, and the public interest permit, all interested parties shall have the opportunity for the submission and consideration of facts, argument, or proposal of adjustment or settlement, without prejudice to any party's rights. No stipulation, offer or proposal shall be admissible in evidence over the objection of any party in any hearing on the matter.

(*b*) Pre-hearing conference.

(1) Prior to any hearing, the CHSB or presiding officer may direct all interested parties, by written notice, to attend one or more pre-hearing conferences for the purpose of considering any settlement under Regulation 4.11(a), formulating the issues in the proceedings and determining other matters to aid in its disposition. In addition to any offers of settlement or proposals of adjustment, there may be considered the following:

(*a*) simplification of the issues;

(*b*) the possibility of obtaining admissions of fact and of documents which will avoid unnecessary proof;

(*c*) limitation on the number of witnesses;

(*d*) the procedure at the hearing;

(*e*) the distribution to the parties prior to the hearing of written testimony and exhibits;

(*f*) consolidation of the examination of witnesses by counsel; and

(*g*) such other matters as may aid in the disposition of the proceedings.

(2) The presiding officer may require, prior to the hearing, exchange of exhibits and any other material which may expedite the hearing. He shall assume the responsibility of accomplishing the purposes of the notice of the pre-hearing conference so far as that may be possible without prejudicing the rights of any party.

(3) In any proceeding under these regulations the presiding officer may call the parties together for an informal conference prior to the taking of any testimony or may recess the hearing for such a conference, with a view to carrying out the purposes of this rule.

*4.14 Conduct of hearings*

(*a*) Presiding officer: powers and duties. The hearing shall be conducted by a presiding officer who shall be a hearing officer designated by the CHSB, or in such cases as the CHSB may determine, by a single member of the CHSB. The presiding officer shall have the authority to arrange and give notice of hearing; sign and issue subpoenas; take or cause depositions to be taken; rule upon proposed amendments or supplements to pleadings; hold conferences for the settlement or simplification of issues; regulate the course of the hearing; prescribe the order in which evidence shall be presented; dispose of procedural requests or similar matters; hear and rule upon motions; administer oaths and affirmations; examine witnesses; direct witnesses to testify or produce evidence available to them which will aid in the determination of any questions of fact in issue, rule upon offers of proof and receive relevant material, reliable and probative evidence; act upon petitions to intervene; permit submission of facts, arguments and proposals of adjustment; hear oral arguments at the close of testimony; fix the time for filing briefs, motions and other documents in connection with hearings; and dispose of any other matter that normally and properly arises in the course of proceedings. The presiding officer or the CHSB may exclude any person from a hearing for disrespectful, disorderly or contumacious language or conduct.

(*b*) Disqualification of presiding officer. Any presiding officer may at any time withdraw if he deems himself disqualified, in which case there will be designated another presiding officer. If a party to a proceeding or his representative files a timely and sufficient affidavit of personal bias or disqualification of a presiding

officer, the CHSB will determine the matter as a part of the record and decision in the case.

(*c*) Objections and exceptions. Formal exceptions to rulings on evidence and procedure are unnecessary. It is sufficient that a party, at the time that a ruling of the presiding officer is made or sought, makes known to the presiding officer the action which he desires taken or his objections to such action and his grounds therefor; provided, that if a party has no opportunity to object to a ruling at the time it is made or to request a particular ruling at an appropriate time, such party, within five (5) days of notification of action taken or refused, shall state his objection and his grounds therefor.

(*d*) Offers of proof. Any offer of proof made in connection with an objection taken to a ruling of the presiding officer rejecting or excluding proffered oral testimony shall consist of a statement of the substance of the evidence which counsel contends would be adduced by such testimony; and if the excluded evidence consists of evidence in documentary or written form or of reference to documents or records, a copy of such evidence shall be marked for identification and shall constitute the offer of proof.

(*e*) Presence of staff members. The names of the members of the CHSB staff present at a hearing, who have been assigned to work on, or to assist in the proceeding, shall be noted in the record.

(*f*) Order of presentation In any hearing held with respect to the revocation of any certification under M.G.L. c. 6 sec. 172, the counsel for the CHSB shall open and close the presentations. Where there is more than one party in the same proceeding, the order of presentation shall be in the discretion of the presiding officer. After all the evidence and testimony of the person opening has been received, the evidence and testimony of all other parties or others who have been allowed to participate in the hearing shall be received in the order determined by the presiding officer. All witnesses shall be subject to examination by the presiding officer, counsel for the CHSB, counsel for other parties, and counsel for any other person as permitted by the presiding officer. A reasonable amount of time for the preparation of cross examination shall be afforded.

(*g*) Conduct of persons present. All parties, counsel, witnesses and other persons present at a hearing shall conduct themselves in a manner consistent with the standards of decorum commonly observed in the courts of this Commonwealth. Where such decorum is not observed, the presiding officer may take such action as he deems appropriate including, but not limited to, the exclusion of any such individuals from further participation in the proceeding.

(*h*) Additional evidence. At any stage of the hearing the presiding officer may call for further evidence upon any issue and require such evidence to be presented by the party or parties concerned or by the counsel for the CHSB either at that hearing or adjournments thereof. At the hearing, the presiding officer may authorize any party to file specific documentary evidence as a part of the record within a specified time.

*4.15 Transcripts*

(*a*) Transcript and record. Of its own accord, the CHSB may provide that all proceedings in a pending matter be officially recorded by a reporter appointed for that purpose at the CHSB's expense. In the event that the CHSB does not so provide, any party may request leave to provide a reporter for the purpose of officially recording the proceeding at its own expense. Such request shall be made to the presiding officer at least three (3) days in advance of the proceeding. In the event that no reporter is present to officially record a proceeding, a sound recording will be made. At the request of any party, the CHSB shall provide a copy of the transcript of the sound recording upon payment of the reasonable cost of preparing said copy. The CHSB need not make said copy available to any party until payment has been received.

(*b*) Transcript corrections. Corrections in the official transcript may be made only to make it conform to the evidence presented at the hearing. Transcript corrections agreed to by opposing attorneys may be incorporated into the record if and when approved by the presiding officer at any time during the hearing, or after the close of evidence, but not more than ten (10) days from the date of receipt of the transcript. The presiding officer may call for the submission of proposed corrections and make disposition thereof at appropriate times during the course of the proceeding. Any objections to the accuracy of the transcript not raised within ten (10) days after the transcript is made available to the objecting party shall be deemed waived.

*4.16 Consolidation*

The presiding officer or the CHSB upon its own motion, or upon motion by a party or other person joined in the proceeding, may order proceedings involving a common question of law or fact to be consolidated for hearing on any or all of the matters in issue in such proceedings.

*4.17 Evidence*

(*a*) The CHSB shall follow the rules of evidence observed by courts when practicable and shall observe the rules of privilege recognized by law, except as otherwise provided by any law. There shall be excluded such evidence as is unduly repetitious or cumulative or such evidence as is not of the kind on which reasonable persons are accustomed to rely in the conduct of serious affairs. All unsworn statements appearing in the record shall not be considered as evidence on which a decision may be based.

(*b*) Official notice may be taken of such matters as might be judicially noticed by the courts of the United States or of this Commonwealth and in addition, the CHSB or the presiding officer may take notice of general, technical, or scientific facts within their specialized knowledge; provided, that the CHSB or the presiding officer shall notify all parties of the material so noticed, and provided further, that any party on timely request be afforded an opportunity to contest the matters so noticed.

(*c*) Documentary evidence; incorporation by reference: CHSB's files. Any matter contained in any records, investigations, reports and documents in the possession of the CHSB of which a party or the CHSB desires to avail itself as evidence in making a decision, shall be offered and made a part of the record in the proceeding. Such records and other documents need not be produced or marked for identification, but may be offered in evidence by specifying the report, document or other file containing the matter so offered.

(*d*) Prepared testimony. The presiding officer may allow prepared direct testimony of any witness to be offered as an exhibit and may omit oral presentation of the testimony. Copies of such proposed exhibit shall be served upon all persons who have filed an appearance and on staff counsel, at least seven (7) days in advance of the session of the proceeding at which such exhibit is to be offered.

(*e*) Stipulations. The parties to any proceeding before the CHSB, by stipulation in writing filed with the CHSB or entered in the record, may agree upon the fact or any portion thereof involved in the controversy, which stipulation may be regarded and used as evidence at the hearing. The CHSB may in such cases require such additional evidence as it may deem necessary.

*4.18 Subpoenas*

(*a*) Issuance. The CHSB and all other parties have authority in accordance with M.G.L. c. 30A sec. 12 to issue subpoenas requiring the attendance and testimony of witnesses and the production of any documents in question in the proceeding. Subpoenas for the attendance of witnesses or the production of documents may be issued without notice to any other party.

(*b*) Motions to quash or modify. Within a reasonable time fixed by the presiding officer, any person to whom a subpoena is directed may petition the presiding officer to revoke or modify a subpoena.

*4.19 Reopening hearings*

No person may present additional evidence after having rested nor may any hearing reopen after having been closed, except upon motion and showing of good cause. Such motions shall be filed with the presiding officer who shall notify all parties of his action upon the motion. Notwithstanding the above, the presiding officer or the CHSB may, at any time prior to the rendering of a decision reopen the hearing on its own motion. In case of such reopening on motion of the presiding officer or CHSB, the parties shall be notified and the hearing shall not be convened less than five (5) days after the sending of such notice.

*4.20 Decisions*

(*a*) Contents and service. All recommended, tentative, and final decisions will include a statement of findings and conclusions as well as the reasons or basis therefor, upon all material issues of fact, law, or discretion presented on the record, and the appropriate relief or denial thereof. A copy of each final decision when issued shall be served on the parties to the proceeding.

(*b*) Filing of presiding officer's recommended decision with the CHSB. The presiding officer shall file his recommended decision together with his statement of findings and conclusions, as well as the reasons or basis therefor, upon all material

issues, fact, law, or discretion presented on the record, and the appropriate relief or denial thereof with the CHBS as soon as practicable after the close of any proceeding.

(*c*) Consideration of presiding officer's recommended decision by CHBS. As soon as practicable after the filing of the presiding officer's recommended decision, the CHSB shall consider the recommended decision of the presiding officer at a duly called meeting.

*4.21 Tentative decisions*

(*a*) Request for a tentative decision. Any party may, in advance of hearing request in writing that the CHSB furnish it a copy of a tentative decision, if a majority of the CHSB has neither heard nor read the evidence. If such a request has been made by any party when a majority of the CHSB has neither heard nor read the evidence, a tentative decision shall be made by the CHSB which may be made on the basis of the presiding officer's recommend decision containing the matters set forth in these regulations. Unless a timely request is filed by a party to a proceeding, the CHSB need not make any tentative decision.

(*b*) Notice of tentative decisions. As soon as practicable after the CHSB has made its tentative decision, the chairman of the CHSB shall forward a copy thereof to any party who is entitled thereto.

(*c*) Filing of objections. A party shall have ten (10) days from the date of mailing of the tentative decision to submit written objections and either oral or written arguments to the CHSB, the choice to be made in the discretion of the CHSB.

*4.22 Oral argument: submission for final decision*

(*a*) Oral argument. If oral argument before the CHSB is desired on objections to a tentative decision, or on a motion or petition, a request therefor shall be made in writing to the CHSB. Any party may make such a request irrespective of his filing objections or written argument. If a brief on objections or argument is filed, the request for oral argument shall be incorporated therein. Applications for oral argument will be granted or denied in the discretion of the CHSB, and if granted, the notice of oral argument will set forth the order of presentation. Those who appear before the CHSB on oral argument shall confine their argument to points of controlling importance raised on objections. Where the facts of a case are adequately and accurately dealt with in the tentative decision, parties should, as far as possible, address themselves in argument to the conclusions.

(*b*) Submission to CHSB for final decision. A proceeding will be deemed submitted to the CHSB for final decision as follows:

(1) if oral argument is had, the date of completion thereof, or if memoranda on points of law are permitted to be filed after argument, the last date of such filing;

(2) if oral argument is not had, the last date when objections or written arguments or replies thereto are filed, or if objections and written arguments are not filed, the expiration date for such objections or written arguments; or

(3) if a majority of the CHSB has neither heard nor read the evidence and a timely request for an opportunity to submit written objections and either written or oral arguments has not been filed, on the date that the presiding officer files his recommended decision with the CHSB.

*4.23 Quorum*

At least a majority of the members of the CHSB shall participate in any action of the CHSB. All decisions and rulings of the CHSB shall be by a vote of a majority of the CHSB present.

*4.24 Appeal from final decision*

The CHSB shall notify all parties of their right to appeal a final decision of the CHSB pursuant to M.G.L. c.30A sec. 14 and M.G.L. c.6 sec. 176 and of the time limit on their right to appeal.

*5.1 Access to records required to be kept by these regulations*

Any record required to be kept by these regulations shall be open only to the CHSB, the Security and Privacy Council, and/or the individual named in the record.

I hereby certify under penalties of perjury that the above drafted document sets forth the regulations approved by the Criminal History Systems Board on December 3, 1974.

ARNOLD R. ROSENFELD,
*Chairman, Criminal History Systems Board.*

## Criminal Offender Record Information System [New]

(Caption editorially supplied.)

### § 167. Definitions

The following words shall, whenever used in this section or in sections one hundred and sixty-eight to one hundred seventy-eight, inclusive, have the following meanings unless the context otherwise requires: "Criminal justice agencies", those agencies at all levels of government which perform as their principal function, activities relating to (*a*) crime prevention, including research or the sponsorship of research; (*b*) the apprehension, prosecution, adjudication, incarceration, or rehabilitation of criminal offenders; or (*c*) the collection, storage, dissemination or usage of criminal offender record information.

"Criminal offender record information", records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation and release. Such information shall be restricted to that recorded as the result of the initiation of criminal proceedings or of any consequent proceedings related thereto. It shall not include intelligence, analytical and investigative reports and files, nor statistical records and reports in which individuals are not identified and from which their identities are not ascertainable.

"Interstate systems", all agreements, arrangements and systems for the interstate transmission and exchange of criminal offender record information. Such systems shall not include recordkeeping systems in the commonwealth maintained or controlled by any state or local agency, or group of such agencies, even if such agencies receive or have received information through, or otherwise participated or have participated in, systems for the interstate exchange of criminal record information.

"Purge", remove from the criminal offender record information system such that there is no trace of information removed and no indication that said information was removed.

Added by St.1972, c. 805, § 1.

1972 Enactment. St.1972, c. 805, § 1, adding this section and sections 168 to 178 of this chapter, was approved July 19, 1972. Section 9 provided: "This act shall take effect conformably to law, except that any agency, department, institution, or individual which is authorized by statute to receive criminal offender record information or which receives the same at the discretion of the commissioner of probation, on the effective date of this act, shall continue to receive the same, notwithstanding any provision of this act to the contrary, until January first, nineteen hundred and seventy-three."

*Cross References*

Correctional institutions,
- Fugitives from justice, descriptions, see c. 127, § 25.
- Identification of prisoners, see c. 127, § 23.
- Department of public safety, criminal information bureau, see c. 22, § 3A.

Fingerprinting and photographing,
- Cities and towns, persons arrested during riots, etc., see c. 41, § 98.
- Persons charged with a felony, see c. 263, § 1A.

Use of systems operated by the board authorized:
- Commissioner of probation, see c. 276, § 100.
- Correctional institutions, see c. 127, §§ 2, 28, 29.
- Department of public safety, see c. 147, § 4A.
- State police, criminal information bureau, see c. 147, § 4C.

### § 168. Criminal history systems board; establishment; members; chairman; terms; meetings; expenses; regulations; powers and duties; director of teleprocessing and other employees; report

There shall be a criminal history systems board, hereinafter called the board, consisting of the following persons: the attorney general, the chairman of the Massachusetts defenders committee, the chairman of the parole board, the chief justice of the district courts, the chief justice of the superior court, the chief justice of the supreme judicial court, the commissioner of the department of correction, the commissioner of the department of public safety, the commissioner of the department of youth services, the commissioner of probation, the executive director of the governor's public safety committee, and the police commissioner of the

city of Boston, or their designees, all of whom shall serve ex officio, and three other persons to be appointed by the governor for a term of three years one of whom shall represent the Massachusetts district attorneys association, one of whom shall represent the Massachusetts chiefs of police association, and one of whom shall represent the county commissioners and sheriffs association. Upon the expiration of the term of any appointive member his successor shall be appointed in a like manner for a term of three years.

The governor shall designate annually the chairman of the board from among its members. No chairman may be appointed to serve more than two consecutive terms. The chairman shall hold regular meetings, one of which shall be an annual meeting and shall notify all board members of the time and place of all meetings. Special meetings may be called at any time by a majority of the board members and shall be called by the chairman upon written application of eight or more members. Members of the board shall receive no compensation, but shall receive their expenses actually and necessarily incurred in the discharge of their duties.

The board, after receiving the advice and recommendations of its advisory committee, shall, with the approval of two-thirds of the board members or their designees present and voting, promulgate regulations regarding the collection, storage, dissemination a usage of criminal ondffender record information.

The board shall provide for and exercise control over the installation, operation and maintenance of data processing and data communication systems, hereinafter called the criminal offender record information system. Said system shall be designed to insure the prompt collection, exchange, dissemination and distribution of such criminal offender record information as may be necessary for the efficient administration and operation of criminal justice agencies, and to connect such systems directly or indirectly with similar systems in this or other states. The board shall appoint, subject to section one hundred and sixty-nine, and fix the salary of a director of teleprocessing who shall not be subject to the provisions of chapter thirty-one or of section nine A of chapter thirty. The board may appoint such other employees, including experts and consultants, as it deems necessary to carry out its responsibilities, none of whom shall be subject to the provisions of chapter thirty-one or of section nine A of chapter thirty.

The board shall make an annual report to the governor and file a copy thereof with the state secretary, the clerk of the house of representatives and the clerk of the senate.

The board is authorized to enter into contracts and agreements with, and accept gifts, grants, contributions, and bequests of funds from, any department, agency, or subdivision of federal, state, county, or municipal government and any individual, foundation, corporation, association, or public authority for the purpose of providing or receiving services, facilities, or staff assistance in connection with its work. Such funds shall be deposited with the state treasurer and may be expended by the board in accordance with the conditions of the gift, grant, contribution, or bequest, without specific appropriation.

Policies, rules and regulations shall not be adopted by the board until a hearing has been held in the manner provided by section two of chapter thirty A.

Added by St. 1792, c. 805, § 1. Amended by St. 1973, c. 961, § 1.

1973 Amendment. St.1973, c. 961, § 1, approved Oct. 29, 1973, added the last paragraph.

1974 Related Laws. St.1974, c. 591, §§ 1, 2, approved July 24, 1974, provided:

"Section 1. Upon control of the computer section at the department of public safety being vested in the criminal history systems board, the employees in the department of public safety whose work is directly related to projects to be administered by the board, shall be transferred to said board.

"Section 2. All employees of the department of public safety who, immediately prior to the effective date of this act, held positions classified under chapter thirty-one of the General Laws or had tenure in their positions by reason of section nine A of chapter thirty of the General Laws and who are hereby transferred to the criminal history systems board, shall be so transferred without impairment of civil service status, seniority, retirement and other rights of the employees, without interruption of their service within the meaning of said chapter thirty-one or said section nine A of said chapter thirty, and without reduction in their compensation and salary grades. All such employees who, immediately prior to the effective date of this act, are not classified under the provisions of said chapter thirty-one, or are not subject to said section nine A of said chapter thirty, shall continue to serve in their respective offices or positions without impairment of their retirement, seniority or other rights and they shall not be lowered in rank or compensation."

**§ 169. Criminal history system advisory committee; establishment; members; vote; chairman; executive secretary, et al.; meetings; powers, duties and functions; participation in interstate system for exchange of record information; reports**

There shall be a criminal history system advisory committee of the board, hereinafter called the advisory committee, consisting of the following persons and their designees: the commissioner of the Boston police department, the attorney general, the commissioner of correction, the commissioner of public safety, the commissioner of youth services, the director of teleprocessing of the criminal offender record system, the executive director of the governor's public safety committee, the president of the Massachusetts district attorneys association, the commissioner of probation, the chairman of the parole board, and the chief justices of the district and superior courts. Each agency represented shall be limited to one vote regardless of the number of designees present at the time any votes are taken.

The advisory committee shall elect its own chairman from its membership to serve a term of one year. No chairman may be elected to serve more than two consecutive terms. The advisory committee may appoint an executive secretary, legal counsel, and such other employees as it may from time to time deem appropriate to serve, provided, however, that such employees shall not be subject to chapter thirty-one or section nine A of chapter thirty.

The chairman shall hold regular meetings, one of which shall be an annual meeting and shall notify all advisory committee members of the time and place of all meetings. Special meetings shall be called at any time by a majority of the advisory committee members, and shall be called by the chairman upon written application of seven or more members.

The advisory committee shall recommend to the board regulations relating to the collection, storage, dissemination and use of criminal offender record information. The advisory committee shall ensure that communication is maintained among the several prime users. The advisory committee shall also recommend to the board the director of teleprocessing of the criminal offender record information system.

The advisory committee may coordinate its activities with those of any interstate systems for the exchange of criminal offender record information, may nominate one or more of its members to serve upon the council or committee of any such system and may participate when and as it deems appropriate in any such system's activities and programs.

The advisory committee may conduct such inquiries and investigations as it deems necessary and consistent with its authority. It may request any agency that maintains, receives, or that is eligible to maintain or receive criminal offender records to produce for inspection statistical data, reports and other information concerning the collection, storage, dissemination and usage of criminal offender record information. Each such agency is authorized and directed to provide such data, reports, and other information.

The advisory committee, shall report annually to the board concerning the collection, storage, dissemination and usage of criminal offender record information in the commonwealth. The board may require additional reports as it deems advisable.

Policies, rules, and regulations shall not be adopted by the advisory committee until a hearing has been held in the manner provided by section two of chapter thirty A.

Added by St.1972, c. 805, § 1. Amended by St.1973, c. 961, § 2.

1973 Amendment. St.1973, c. 961, § 2, approved Oct. 29, 1973, added the last paragraph.

**§ 170. Security and privacy council; establishment; members; chairman; terms; clerical assistance; meetings; duties and functions; expenses; reports; participation in interstate system for exchange of record information**

There shall be a security and privacy council, hereinafter called the council, consisting of the chairman and one other member of the advisory committee, chosen by the advisory committee, and seven other members to be appointed by the governor, to include representatives of the general public, state and local government, and one representative of the criminal justice community. Of the seven members initially appointed by the governor, two shall be appointed for a

period of one year, two shall be appointed for a period of two years, two shall be appointed for a period of three years, one shall be appointed for a period of four years. Thereafter, each of the appointments shall be for a period of four years. Each member appointed by the governor shall serve until his successor is appointed and has qualified. The chairman of the council shall be elected by and from within the council to serve for a term of two years. The advisory committee shall provide such clerical and other assistance as the council may require. The council shall meet at the call of the governor, its chairman, or any three of its members and shall conduct a continuing study and review and to make recommendations concerning questions of individual privacy and system security in connection with the collection, storage, dissemination, and usage of criminal offender record information. Council members shall receive no compensation for their services on the council but shall receive their expenses necessarily incurred in the performance of official duties.

The council may conduct such inquiries and investigations as it deems necessary and consistent with its authority. The board, each criminal justice agency in the commonwealth, and each state and local agency having authorized access to criminal offender record information, is authorized and may furnish to the council, upon request made by its chairman, such statistical data, reports, and other information directly related to criminal offender record information as is necessary to carry out the council's functions.

The council shall make an annual report to the governor and file a copy thereof with the state secretary and the clerk of the house of representatives and the clerk of the senate. It may make such additional reports and recommendations as it deems appropriate to carry out its duties.

The council shall appoint one or more of its members to serve upon any similar council or committee connected with any interstate system for the exchange of criminal offender record information, and may participate as it deems appropriate in the activities of any such system.

Policies, rules and regulations shall not be adopted by the council until a hearing has been held in the manner provided by section two of chapter thirty A.

Added by St. 1972, c. 805, § 1. Amended by St. 1973, c. 961, § 3

1973 Amendment. St. 1973, c. 961, § 3, approved Oct. 29, 1973, added the last paragraph.

**§ 171. Regulations generally; continuing educational program**

The board shall promulgate regulations (*a*) creating a continuing program of data auditing and verification to assure the accuracy and completeness of criminal offender record information; (*b*) assuring the prompt and complete purging of criminal record information, insofar as such purging is required by any statute or administrative regulation, by the order of any court of competent jurisdiction, or to correct any errors shown to exist in such information; and (*c*) assuring the security of criminal offender record information from unauthorized disclosures at all levels of operation.

The board shall cause to be initiated for employees of all agencies that maintain, receive, or are eligible to maintain or receive criminal offender record information a continuing educational program in the proper use and control of such information.

Added by St. 1972, c. 805, § 1.

**§ 172. Dissemination of record information to authorized agencies and individuals; determination of eligibility for access; certification; listing; scope of inquiry; regulations; access limited; authorization**

Criminal offender record information shall be disseminated, whether directly or through any intermediary, only to (*a*) criminal justice agencies and (*b*) such other individuals and agencies as are authorized access to such records by statute.

The board shall certify which agencies and individuals requesting access to criminal offender record information are authorized such access. The board shall, regarding such agency or individual, make a finding in writing of eligibility or non-eligibility for such access. No such information shall be disseminated to any agency or individual prior to the board's determination of eligibility or, in cases in which the board's decision is appealed, prior to the final judgment of a court of competent jurisdiction that the agency or individual is so eligible.

Each agency holding or receiving criminal offender record information shall maintain, for such period as is found by the board to be appropriate, a listing of

the agencies or individuals to which it has released or communicated such information. Such listings, or reasonable samples thereof, may from time to time be reviewed by the board, advisory committee, or council to determine whether any statutory provisions or regulations have been violated.

Dissemination from any agency in this commonwealth of criminal offender record information shall, except for purposes of research programs approved under section one hundred and seventy-three, be permitted only if the inquiry is based upon name, fingerprints or other personal identifying characteristics. The board shall promulgate regulations to prevent dissemination of such information, except in the above situations, where inquiries are based upon categories of offense or data elements other than said characteristics.

Notwithstanding the provisions of this section, access to criminal offender record information on the basis of data elements other than personal identifying characteristics shall be permissible if the criminal justice agency seeking such access has first obtained authorization from the commissioner of probation, or in his absence, a deputy commissioner of probation. Such authorization may be given as a matter of discretion in cases in which it has been shown that such access is imperative for purposes of the criminal justice agency's investigational or other responsibilities and the information sought to be obtained is not reasonably available from any other source or through any other method.

Added by St.1972, c. 805, § 1.

**§ 173. Regulations for program research; monitoring; access restricted**

The board shall promulgate regulations to govern the use of criminal offender record information for purposes of program research. Such regulations shall require preservation of the anonymity of the individuals to whom such information relates, shall require the completion of nondisclosure agreements by all participants in such programs, and shall impose such additional requirements and conditions as the board finds to be necessary to assure the protection of privacy and security interests.

The board may monitor any such programs to assure their effectiveness. The board may, if it determines that a program's continuance threatens privacy or security interests, prohibit access on behalf of any such program to criminal offender record information.

Added by St.1972, c. 805, § 1.

**§ 174. Interstate system for exchange of record information; supervision of participation by state and local agencies; access limited; telecommunications access terminals**

The board shall supervise the participation by all state and local agencies in any interstate system for the exchange of criminal offender record information, and shall be responsible to assure the consistency of such participation with the terms and purposes of sections one hundred and sixty-eight to section one hundred and seventy-eight, inclusive.

Agencies at which criminal offender records are sought to be inspected shall prescribe reasonable hours and places of inspection, and shall impose such additional restrictions as may be approved by the board, including fingerprinting, as are reasonably necessary both to assure the record's security and to verify the identities of those who seek to inpect them.

Added by St.1972, c. 805, § 1.

**§ 176. Appeal; de novo hearing; equitable relief**

Any individual or agency aggrieved by any order or decision of the board or adverse recommendation of the council or failure of the council to issue findings may appeal such order, recommendation or decision to the superior court in the county in which he is resident or in which the board issued the order or decision from which the individual or agency appeals. The court shall in each such case conduct a de novo hearing, and may order such relief as it finds to be required by equity.

Added by St.1972, c. 805, § 1.

**§ 177. Violations; civil liability**

Any aggrieved person may institute a civil action in superior court for damages or to restrain any violation of sections one hundred and sixty-eight to one hundred and seventy-five, inclusive. If it is found in any such action that there has occurred a willful violation, the violator shall not be entitled to claim any priv-

ilege absolute or qualified, and he shall in addition to any liability for such actual damages as may be shown, be liable for exemplary damages of not less than one hundred and not more than one thousand dollars for each violation, together with costs and reasonable attorneys' fees and disbursements incurred by the person bringing the action.

Added by St.1972, c. 805, § 1.

**§ 178. Violations; punishment**

Any person who willfully requests, obtains or seeks to obtain criminal offender record information under false pretenses, or who willfully communicates or seeks to communicate criminal offender record information to any agency or person except in accordance with the provisions of sections one hundred and sixty-eight to one hundred and seventy-five, inclusive, or any member, officer, employee or agency of the board, the advisory committee, the council or any participating agency, or any person connected with any authorized research program, who willfully falsifies criminal offender record information, or any records relating thereto, shall for each offense be fined not more than five thousand dollars, or imprisoned in a jail or house of correction for not more than one year, or both.

Added by St.1972, c. 805, § 1.

---

## Legal Memorandum on Department of Justice Regulations on Criminal Justice Information Systems, Federal Register, May 20, 1975

### Subpart C: Sections 20.30–20.38

office of the attorney general, commonwealth of massachusetts

### I. The New Department of Justice Regulations for Criminal Records Violate Constitutional Rights

The new regulations for the CCH program[1] and related manual systems infringe upon basic constitutional guarantees. The present operating policies intended to control file content, access to the files, updating and purging procedures, and rights to individual notice and challenge are so lax as to permit and encourage violations of rights protected by the First, Fourth, Fifth, Sixth, Eighth, Ninth, Tenth and Fourteenth Amendments of the United States Constitution.

The Computerized Criminal History program was established to provide a national index of criminal offender records in order to expedite the identification and processing of criminal suspects. The system consists of identification and criminal history data—from arrest through court and correction stages—of all persons arrested for a "serious or significant" crime in any state or federal jurisdiction participating in the system. Through access by computer terminal to the national file, criminal justice agencies in all participating states will have immediate notice of the complete criminal history of any person, no matter how many states that history might involve

At present, the system is not fully operational. Although ten federal agencies introduce data into and withdraw data from the file[2] only four states[3] and the District of Columbia are full participants. As of March 1, 1975, the system contained only 549,595 CCH files. However, it is projected that by 1983 as more states join the system and enter their records into the national files, there will be eight million files.

There are in addition currently 60 million fingerprint files maintained by the FBI Identification Division, on 21 million individuals[4] obtained from local and state arrest "rap sheets" which can and are used in place of the automated system.

The vast fingerprint file maintained by the FBI and the limited current operation of the system and its projected enormous expansion lead to two conclusions. First, although the infringement of Constitutional rights outlined below is presently of grave concern, the problem will become even more serious as the system expands. Second, the opportunity is especially good at present to prevent such violations by requiring the Justice Department to promulgate amended regulations that address these serious issues, rather than give formal status to the

[1] 40 Fed. Register, 22115 (May 20, 1975).

[2] These agencies are: FBI, Dept. of Justice, Bureau of Customs, Provost Marshal General of the Army, Naval Investigations, Office of Special Investigations (Air Force), Marine Corps, Secret Service, Postal Investigation Service and Bureau of Prisons.

[3] Arizona, California, Florida, Illinois.

[4] GAO Audit, "How Criminal Justice Agencies Use Criminal History Information" B-171019 (Aug. 19, 1974).

existing system's weaknesses. This is the principal deficiency of the recently adopted regulations. They do not correct existing abuses but rather codify procedures which have always been Constitutionally deficient.

As presently operated and conceived, the major problems of the CCH system are overly broad access to offender records and lack of control over the accuracy of file contents. As the Report of the Secretary's (HEW) Advisory Committee stated:

"NCIC is essentially an automated receiver, searcher, and distributor of data furnished by others. If a subscribing system enters a partially inaccurate record or fails to submit additions or corrections to the NCIC files (e.g., the recovery of a stolen vehicle or the disposition of an arrest), there is not much that the NCIC can do about it.

"Furthermore, the risk of propagating information that may lead to unjust treatment of an individual by law enforcement authorities in subscribing jurisdictions cannot be fully prevented." (p. 18)

The current regulations do not correct this situation. Indeed they institutionalize it. See 28 C.F.R. 20.31.

### A. INCLUSION AND DISSEMINATION OF ARREST RECORDS

As presently operated, the NCIC/CCH system provides no assurance that once a file is created on an individual, its entries will be complete. The system contemplates "cycles" of information, each cycle being initiated by an arrest record and then updated by entries indicating disposition of the arrest in the courts and corrections phases of the criminal justice system.[5] Accordingly, the regulations provide that "Criminal history record information means information collected in criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision and release," 28 C.F.R. 20.3(b).

However, experience indicates that information beyond the arrest stage is rarely entered into the files, thereby leaving the files replete with arrests that did not result in conviction, or even prosecution, but which are not so designated. Section 20.37 requires only that contributing agencies submit dispositions "to the maximum extent feasible . . . within 120 days after the disposition has occurred."

Such records serve no legitimate law enforcement purpose and instead can cause serious detriment to the individual. As the Supreme Court stated in Schware v. Board of Bar Examiners, 353 U.S. 232, 341 (1957):

"The mere fact that a man has been arrested has very little, if any, probative value in showing that he has engaged in any misconduct. An arrest shows nothing more than that someone probably suspected the person apprehended of an offense."

Section 20.33 authorizes broad dissemination of arrest data without disposition up to one year after an arrest followed by no active prosecution. The only privacy safeguard is forbidding dissemination after that one year period if no disposition has been noted.

The detrimental effects of including incomplete arrest data in the CCH file and the Identification Division of the FBI occur both within the criminal justice system and in regard to other agencies and institutions. At present, full CCH records and Identification Division records are broadly disseminated among all agencies of the criminal justice system without limitation. This means that a sentencing judge, for example, can be swayed by an inaccurate arrest record, even when it has no bearing upon the crime in question. Similarly, probation and parole boards are negatively influenced by incomplete arrest records and lack the means to determine on their own whether the arrest led to a conviction. Employment in the criminal justice system becomes almost impossible because of the suspicion of alleged criminal conduct which was never proved in a court.

Of even greater significance is the damage done to individuals by the distribution of incomplete records to prospective employers in both the public and private sectors. The NCIC files are routinely made available to federal agencies, and to many private employers that are licensed or regulated by the states. There is evidence that arrest records that did not result in convictions or that were totally unrelated to the job sought by the applicant are frequently the cause of applicant rejection and loss of employment opportunity.[6]

---

[5] National Crime Information Center, Computerized Criminal History program background, concept and policy as approved by NCIC Advisory Board (Sept. 20, 1972).

[6] *Menard v. Saxbe*, 498 F. 2d. 1017 (D.D.C. 1974).

Section 20.33 authorizes wide access to criminal records, including arrests not followed by conviction up to one year old, to criminal justice agencies, federal agencies authorized by statute or Executive Order and pursuant to PL. 92–544 (86 Stat. 115) for use in connection with licensing or local/state employment or for other uses only if such dissemination is authorized by federal or state statute and approved by the U.S. Attorney General. In effect, there are few if any restrictions on such access for federal agencies. Criminal charges followed by dispositions including "innocent," "acquitted," "dismissed," and "continued without a finding" may be disseminated to all eligible recipients under these regulations.

Recent court decisions have recognized the serious violations of constitutional rights that can flow from the dissemination of arrest records. In *Menard* v. *Saxbe*, 498 F. 2d. 1017 (D.D.C. Cir. 1974), the Court enjoined the distribution of most arrest records, because of the serious consequences to the individual of broader, uncontrolled dissemination to state agencies, or private employers. In an earlier version of the same case, the court concluded that the NCIC was "out of effective control." The court stated that "the overwhelming power of the Federal Government to expose must be held in proper check." *Menard* v. *Mitchell*, 328 F. Supp. 718, 726 (D.D.C. 1971).

While individual rights are most seriously threatened by widespread dissemination of records of arrests not resulting in conviction, the courts have suggested that they are also violated by the mere retention of such records in the police files. In *United States* v. *Hudson*, A. 2d, 43 U.S.L.W. 2377 (D.C. Super. Ct., Feb. 19, 1975) the court ordered expungement of arrest data:

"The right to privacy has been described as the individual's ability to control information about himself. He loses such ability when through an arrest the government obtains data about him which it would not normally secure."

Two earlier state court decisions have held that the arrest record of a person acquitted of a crime should be expunged when the state is unable to make a compelling showing of the necessity to retain the record sufficient to outweigh the person's fundamental right of privacy. (*Eddy* v. *Moore*, 5 Wash. App. 334, 487 P. 2d 211 (1971); *Davidson* v. *Dill* — Colo. —, 503 P. 2d 157 (1972)). The *Eddy* court noted:

"The value of fingerprints and photographs of an arrested person depends upon two factors: an assumption the individual arrested did, in fact, commit the crime for which he is accused, and that his commission of this crime indicates a likelihood that other crimes will be committed. An acquittal seems to negate both premises." (at 217)

### B. PERIODIC REVIEW AND EXPUNGEMENT OF CERTAIN ENTRIES.

The regulations abdicate the FBI of all responsibility for the accuracy of the criminal offender files it maintains and disseminates. Section 20.34(b) states: "If, after reviewing his identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections or updating of the alleged deficiency, he must make application directly to the contributor of the questioned information. *If* the contributor corrects the record, it shall promptly notify the FBI and, upon receipt of such a notification, the FBI will make any changes necessary. . . ."

There are no provisions for the routine purging of outdated data pursuant to state law of the contributing agency by the NCIC. Thus, states which have strict purging requirements cannot be assured that their law will be followed.

The denial of due process and privacy in the collection, retention, and dissemination of inaccurate, incomplete and outdated records, which is permitted by the regulations cannot be offset by the claim that retention is necessary for effective law enforcement. The NCIC's purpose is to provide ready access to data on past criminal offenders. Inclusion of inaccurate records can only mislead the system's users; inclusion of records on persons who are, in fact, non-criminals can only clutter the system. In both cases, the record subject suffers grave injury.

In *U.S.* v. *Mackey*, —— F. Supp. ——, 43 U.S.L.W. 2333 (D.C. Nev. Jan. 27, 1975) a federal district court called an erroneous NCIC report "a capricious disregard for the rights of the defendant as a citizen," and concluded that the evidence seized as an arrest based on such inaccurate information must be suppressed. The inaccurate NCIC listing, in the view of the court, made the defendant a "marked man, subject to being deprived of his liberty, at any time and without any legal basis."

Further, retention and dissemination of outdated conviction data provides a bar to effective rehabilitation of ex-offenders precluding them from jobs and other necessities.

C. CONTROL OVER PRIMARY AND SECONDARY ACCESS TO FILES

Even if the NCIC records were accurately and adequately maintained, the absence of proper controls on access to those records would present a serious violation of the file subjects' rights to privacy and due process. While the FBI attempts to limit primary or direct access to NCIC records to law enforcement and specified, non-criminal justice agencies, it repudiates all responsibility for secondary access (access by users who are not themselves criminal justice agencies but who seek information through such agencies). (Section 20.36 provides that agencies with direct access should abide by present NCIC regulations. Other than banishment from the system, there are no sanctions to enforce this provision.)

Section 20.36 proclaims that direct inquiries to the NCIC records will be permitted only for criminal justice agencies, that "execute a signed agreement with the Director." Any assumption that this policy will work to restrict the number of authorized inquirers into the system is mitigated by the prior statement in the NCIC Policy Paper that the "NCIC system . . . has a potential of over 45,000 local, state and Federal criminal justice terminals.[7] Any inquiry which comes in from any of these 45,000 user-terminals is automatically answered by the computers, and it is presumed to be a request properly within the official mandate of the user-agency without further check into the authority and motives of the terminal operator or the eventual recipient of the data.[8]

Section 20.33 (a) (1) does state that file data should be disseminated only for criminal justice purposes. However, this does not preclude the dissemination of such data for use in connection with licensing or local or state employment, other than with a criminal justice agency. Section 20.33 (a) (2) and (3) allows dissemination to Federal agencies authorized by statute or Executive Order; and for licensing or local or state employment or for other uses only if such dissemination is authorized by federal, state law and approved by the Attorney General. There are no standards for the Attorney General's approval, however.

By adopting such a broad proviso, the FBI abdicates all possible control over secondary access to and use of NCIC criminal history files. In so doing, it may be in violation of the statute under which the NCIC claims to operate, which permits exchange of records with and for the official use of authorized officials but makes such exchange subject to cancellation "if dissemination is made outside the receiving departments or related agencies." Further, such provision abandons all attempts to construct a uniform, national system which maintains proper respect for the rights of privacy, due process, equal protection, and fairness of persons who properly or improperly become subjects of an NCIC file. Such rejection of uniformity makes the whole system as vulnerable to misuse as the most lenient state or Federal standard. The Justice Department had the opportunity to create such a national standard with its new Regulations. Its failure to do so in effect nullifies any benefits arising from the promulgation of the Regulations.

*Role of the states*

While the NCIC Policy Paper claims that "(e)ach record, for all practical purposes, remains the possession of the entering agency," [9] that claim is patently false. Section 20.31 defines NCIC/CCH as a "central repository" as well as an "index" for the states and other contributing agencies. A state with proper concern for the rights of its citizens—which by statute severely restricts the uses of criminal records and imposes real sanctions for violations such as Massachusetts, Washington, and Iowa—surrenders its citizens to the abuses permitted by the lowest standard of the fifty states, the federal government or any one of the 45,000 terminals. For this very reason, Massachusetts has refused to join the NCIC system. In a June 13, 1973 letter to the Attorney General, Francis W. Sargent, then Governor of Massachusetts, wrote:

". . . I take very seriously the President's Commission's warning that the application of computer technology for criminal justice information requires special precautionary steps to protect individual rights. The Massachusetts criminal information system has been designed to provide internal and external safeguards against potential abuse. Unfortunately, I have seen no similar action on the part

[7] National Crime Information Center, Computerized Criminal History System, concept and policy as approved by the NCIC Policy Board (Sept. 20, 1972) at 3.

[8] The Report of the Secretary's (HEW) Advisory Committee put the problem this way: "The ease with which inquiries can be made from remote terminals located in law enforcement and criminal justice agencies all over the country could lead to access to the NCIC criminal history files by more users and for checking on more individuals than is socially desirable." (p. 17).

[9] NCIC Policy Paper, supra, Note 7 at 3.

of the Department of Justice, the Attorney General or the Federal Bureau of Investigation to construct equivalent safeguards for the national criminal information system."

Several other states have also declined to participate in the NCIC/CCH including New York and Pennsylvania.

Failure of the FBI to adopt uniform minimum standards which are not so loose as to permit the abuse of Constitutional rights, or to enact adequate sanctions or to recognize the pre-eminence of state law over data and improper use of the system pertaining to citizens of these states, cannot be justified. No state that is unwilling or unable to conform to operating standards—prescribed in Subpart B of the Regulations which assure protection of constitutional rights—should be permitted to join or remain in the NCIC system.

Section 20.31 includes the FBI Identification Division as part of the NCIC/CCH system for the first time. The Identification Division is supposed to maintain the fingerprint file for the entire NCIC/CCH system. In addition, the manual reports in the Identification Division will be merged with the automated records currently in the CCH file. Since a number of states have refused to participate in the CCH file, the merger of the records will permit the merger of records from those states into the CCH file against their will. This will result because all states participate in the Identification Division fingerprint and other systems. When they provided the records however, they did not anticipate that such records might become part of the inadequately protected automated federal/state CCH system. In effect, the regulations permit an endrun around the intentions of such states, an endrun which is detrimental to the cause of privacy and subversive of the Tenth Amendment to the U.S. Constitution.

This Amendment which protects the sovereignty of the States is supposed to protect against invasion of state power by the Federal government. Removing the ability of a state to control its criminal records according to its interpretation of Constitutional requirements seems to be the kind of abuse which the Tenth Amendment is designed to protect against.[10]

### D. INDIVIDUAL ACCESS AND REVIEW/CORRECTION.

Although section 20.34 allows an individual access to his files, it fails to provide any requirement that incorrect data must be corrected by the NCIC, except upon request of a contributing agency. The result is an undue burden on the individual, making it virtually impossible for the individual to correct incorrect data already accessed from the NCIC and Identification Division. Section 20.21 mandates that state criminal justice information systems shall notify agencies given incorrect data. There is no such requirement for the NCIC although the data is the same. Thus, a record may be corrected after the effects of its having been disseminated have already occurred.

### E. SPECIFICATION OF CRIMES INCLUDED IN NCIC

Section 20.32 of the Regulations requires that data in criminal history files "be restricted to serious and/or significant violations." The guidelines specify a number of crimes that are to be excluded from the system, but there is no specific statement of those that are to be included. The determination of which criminal acts are serious or signific nt enough to warrant inclusion in the national file is left with each individual state, and no attempt is made to guide that choice to assure that the categories chosen are reasonably limited or uniform among the States.[11] Subpart B does not limit file content on state systems other than restricting inclusion of juvenile records. (See Section 20.21(d).) As a result, the system as currently designed will accept data on at least 423 offenses, and excludes only 14 offenses as insignificant.[12] In some jurisdictions domestic relations crimes such as nonsupport and nonpayment of alimony, and victimless crimes such as homosexuality, gambling, and others are considered "serious" and may be included in NCIC files. Narcotic and mental commitment records are maintained in the

---

[10] *NAACP v. Thompson*, 357 F. 2d. 831 (5th Cir. 1966), Art. den. 385 U.S. 280.

[11] "In the last analysis only the contributing agencies can determine if a particular charge is significant enough to be included in the national file," is the explanation for abdication of federal responsibility provided in "NCIC—A Tribute to Cooperative Spirit," *FBI Law Enforcement Bulletin*, February 1972.

[12] "National Crime Information Center Uniform Offense Classifications." This document details the codes necessary to enter records in the CCH files. On its four pages are listed 437 crimes, divided among 48 categories, each crime carrying a computer code number. Of the 437 crimes, only 14 are designated as "not to be entered in National Index," those 14 being basically the ones enumerated.

national file if they are part of the criminal justice process. Moreover, any State or locality may store additional information in its state level files, which can be disseminated upon requests referred to it by the CCH central file.

Further, section 20.31(c) grandfathers all existing records in the Identification Division. Considering the vast number of such files, this represents a significant exemption of records, many of which are likely to be inaccurate or incomplete. This inclusion of existing crime categories does not conform with the stated purpose of the CCH file of "contending with increasing criminal mobility or recidivism."[13] Many of the crimes included in the file are generally local offenses of little relevance to regional or national interest. The broad listing does not achieve the desired goal of a nation l system consisting of truly serious crimes. In addition, beyond the failure to limit the system to the needs that allegedly justified its creation, the system is deficient because of its vagueness. Despite the serious detriments in terms of employment and other opportunities that frequently result from inclusion of a subject in the national files—thereby increasing the penalty for criminal conduct—there is virtually no way an individual can determine whether an offense is sufficiently "serious" to be included in the national file.

While the current list of 423 offenses might be considered as establishing the outer limits of nationally recordable conduct, there is no uniformity of practice among the states. Inclusion of his record in a national file is far more detrimental to an individual than inclusion only in the files of the one state in which he had contact with the criminal justice system, because of the vast increase in dissemination of his criminal history which results. If such a national file did not exist, a person or organization wishing to construct the subject's criminal history would have to canvass the fifty states individually. It is unlikely that such a procedure would be undertaken except under the most compelling circumstances, : nd thus interstate dissemination would be limited

Although states may limit file content, there is nothing in the regulations to indicate that contributing Federal agencies will conform to state law when entering data on state offenders from such a state. As a result, the state cannot be assured that its laws are being upheld or even that its records are being treated in a manner consistent with the requirements of its laws. For example, Section 20.24 which indicates that the receiving state "may" comply with the sending state's sealing or purging statutes.

### F. CONTROL OVER LAW ENFORCEMENT TELECOMMUNICATION LINES AND MESSAGE SWITCHING FACILITIES

These regulations go beyond any statutory authorization granted to the FBI to control telecommunication lines and message switching facilities linking local, state and federal criminal justice agencies.

The authority which appears in Section 20.31 declares that the "FBI Shall operate the National Crime Information Center (NCIC) the computerized information system which includes the telecommunications lines and any message switching facilities which are authorized by law or regulation to link local, state and Federal criminal justice agencies for the purpose of exchanging NCIC-related information." The potential effect of this regulation is to permit the FBI to absorb all state and local justice data systems with the creation of a national police data communication system.

The proposal has been severely criticized by the Law Enforcement Assistance Administration, the White House Office of Telecommunications Policy and the Domestic Council Committee on the Right of Privacy.[14] Nonetheless the proposal appears in the approved draft of the regulations. It apparently reflects the attitude of the FBI that "security and privacy considerations are not of primacy concern to the FBI in its development of the computerized criminal history program."[15]

Further, this represents another serious intrusion into local policing and other matters outside the jurisdiction of the FBI and in violation of the FBI's authorized mission.

Senator TUNNEY. Thank you very much, Mr. Bellotti. Our next witness is Mr. Paul K. Wormeli, vice president of Public Systems, Inc., Sunnyvale, Calif., and a former national project director for Project SEARCH.

---

[13] NCIC Policy Paper, supra, Note 7.
[14] Burnham, "FBI's Data Plan Scored by Agency," *New York Times*, June 4, 1975 at 25.
[15] FBI response to LEAA criticism quoted in *Id.*

Mr. Wormeli, I know it is a difficult thing to do, but I am going to ask you, if you could, sir, to summarize your statement. I have a bill that is coming up on the floor in another few minutes, one that I cosponsored with Senator Hollings. He is going to make the initial statement, and I have to get over there in 20 minutes. I want to be able to ask you a few questions. If you could summarize your testimony, maybe in 5 to 10 minutes, it will give me a chance to direct specific questions to you.

## TESTIMONY OF PAUL K. WORMELI, VICE PRESIDENT OF PUBLIC SYSTEMS, INC., SUNNYVALE, CALIF., AND FORMER NATIONAL PROJECT DIRECTOR OF PROJECT SEARCH

Mr. WORMELI. Mr. Chairman and members of the subcommittee, I wish to thank you for your invitation to appear before you to comment on S. 2008. My remarks will be based on my experiences in a number of national projects dealing directly with this issue. The effective and proper use of criminal history information has occupied a great deal of my time during the past 6 years.

My company works exclusively in the field of law enforcement and criminal justice and I speak with sympathy for the more informed law enforcement agencies throughout the country.

First, let me say that I believe S. 2008 to be a distinctive step forward in the legislative deliberations regarding criminal history information. This bill is, as the chairman has stated, a much clearer and precise coverage of the issues than has been afforded by earlier proposed legislation. I strongly believe that the provisions of S. 2008 provide the basic protections of individual privacy while at the same time preserving the right of law enforcement and criminal justice agencies to obtain the data necessary for their effective operations.

Rather than pursue the rhetoric which can go on forever, let me just make one comment about the need for this data as well as the need for privacy.

To begin to deal with improving the administration of justice, it is imperative that we begin to understand the flow of individuals through the criminal justice system, and that we provide the data needed by law enforcement officers and other officials in a timely and accurate fashion.

There is no other way to properly plan for the improvement of the system than by examining the performance of the system in terms of its common element; namely, the persons to whom the criminal justice sanction is being applied.

At this point, I would claim that the lack of legislative action to date has been an impediment to progress in this field. Many State and local governments have been unwilling to move forward to provide this necessary data to criminal justice agencies because of the lack of agreement at the Federal level as to what standards will be imposed on handling criminal history information. Without some end to this confusion, governmental agencies throughout the country will not commit themselves to providing the tools required by law enforcement. I believe that most people in the criminal justice community are now at the point where they would be relieved by any action by the Congress, regardless of the nature of that action.

Basically, I find myself in complete agreement with most of the provisions of S. 2008. There are a number of specific technical problems which I am sure will be discussed by other speakers and introduced into the hearings and have already been discussed with the staff.

As far as I can tell, the provisions of the bill are mostly in accord with the position repeatedly taken by Project SEARCH which is, as you know, a national consortium of 50 States of experienced individuals in this field representing the criminal justice community. Their opinion and their deliberations on these matters should carry far more weight than an individual like myself.

I would now like to briefly comment on two specific provisions. With respect to the sections of the bill dealing with the use and dissemination of these records, I would urge the subcommittee to keep in mind that the abuses which have occurred in the use of criminal history information have been primarily related to uses by organizations and individuals not performing criminal justice duties. The basic purpose of collecting this data is to help criminal justice agencies do their job. I believe the bill provides adequate controls on the use of these records by law enforcement and criminal justice agencies.

It is important to everyone concerned about these issues that the abuses in the use of this information for employment purposes be brought to a halt.

When you boil everything else down, the major concern to the criminal justice community as well as to the public and to the individuals involved in these systems is the security and accuracy of the information. Much of the fear associated with the use of these files would be eliminated if the agencies keeping the records could assure everyone that the records are complete and accurate, which is certainly not the case with the existing manual systems.

The provisions of section 208 which call for the sealing and purging of arrest information are overly restrictive. There are many instances in which officers need arrest records to do their jobs. In view of the fact that abuses of this data have not been attributable to the law enforcement agencies and because of the influences outside the control of the law enforcement agencies regarding potential prosecution, it would appear to me that the controls over dissemination of arrest information would suffice to protect individual privacy.

One other point in the bill that I wish to comment on is the definition of material which can be contained in a computerized intelligence index. I strongly believe that such an index can legitimately contain data taken from public records—ownership of corporations and other public documents—and that such data can be a baseline for the common investigations undertaken by numerous law enforcement agencies, particularly in the field of organized crime. I see no gain by excluding such public record data from a computerized index available to the agencies involved in a particular case.

I would now like to turn to several issues which are not contained in S. 2008, and urge your consideration of these additional points.

One of the issues of great concern to State and local governments is the authority and the limits on activity to be granted to the Federal Bureau of Investigation in its operation of the National Crime Information Center. Criminal justice officials throughout the Nation rely on many of the services of the National Crime Information Center. Yet, there has never been a clear definition of the services which the FBI should provide to State and local governments.

For the last 5 years, substantial debate has ranged throughout the executive branch of the Federal Government, involving a great deal of time and causing substantial confusion in the minds of the criminal justice officials who seek to work out agreements between the FBI and their own governments as to responsibilities for the collection, preservation, and dissemination of criminal history information.

I am convinced that policy legislation on this matter is the only way to resolve the confusion. The debate over whether or not the FBI should provide message-switching services as opposed to a consortium of States created to provide such a national service, appears to be irresolvable in the executive branch of Government. Through a succession of Attorneys General, different points of view have been aired, without any final resolution. I strongly believe that the only way to solve this problem and eliminate the confusion is for the Congress to specifically proscribe the services which the FBI should provide to local agencies.

I believe these issues are not irresolvable, and that this current bill is a logical place to delimit the functions of the FBI with respect to criminal history information as well as other information exchange and telecommunication services. Senator Hruska pointed out over a year ago, as did other members of the subcommittee, that the Congress should make this decision. I believe the Congress should, and I think this bill is the place to do it.

There is a second issue of concern to State and local officials, as was mentioned by Attorney General Bellotti, and that is the relationship of this bill to the regulations recently issued by the Department of Justice.

There is one controversial section in those regulations dealing with the requirement for States to dedicate computer systems to criminal history information. As I am sure you know, Senator, the issue of dedicated versus shared systems has been debated as long as the issue of privacy in this field. Those of us who have been actively involved in the criminal justice field for some time support the concept of dedication on the ground that the responsiveness the criminal justice system needs demands their own system. Project SEARCH, as far back as 1970, endorsed the general principle of dedicated computer systems for the storage of criminal history information. However, the data processing officials have argued that such approach is costly and no technologist I know will dispute that claim.

I do believe the responsiveness need for data outweighs the economic arguments against dedicating these systems. At the same time, however, I do not believe that the security and privacy arguments are a sound basis for insisting upon dedication. Therefore, I would suggest that there be some consideration given to the Department of Justice regulations and whatever revisions you might wish to make through this bill. It would have been preferable for the Department of Justice to define the levels of security to be provided by any system, regardless of whether it is shared or not rather than to impose a particular solution.

Dedication of a system in its own right does not guarantee privacy or security. It is an intuitive attempt to promote improved privacy and security. I would propose that this present bill either repeal that particular section of the Department of Justice regulations which deal with dedication or considerably narrow its scope to limit the

coverage to repositories developed at the State level for criminal history information.

I would go on to say that the remaining parts of the Department of Justice regulations, in particular subpart B, are sound first steps in improving the accuracy and completeness of criminal history information systems and in controlling the uses of such systems. In fact, your bill uses much of the same language as the regulations contain. It would seem appropriate to complete S. 2008 with a reference to these regulations as a first attempt upon which the Commission mentioned in title 3 will build.

Some notation of the existence of these regulations and support for their existence, particularly subpart B, would further integrate the development of improved procedures in this field.

Thank you very much.

Senator TUNNEY. Thank you very much.

I would like to ask you about a few of the specific complaints that were voiced by Chief Pomerance and get your evaluation of those complaints.

He said, and I am quoting from his testimony, "We believe that S. 2008 unnecessarily imposes upon State and local agencies standards dictated by the Federal Government, which would grant the Commission the ability to control the day-to-day details of State and local criminal justice administration."

Mr. WORMELI. I do not believe this provides that opportunity. My reading is that it provides a set of basic standards for all States to adopt and then turns around and gives the complete control back to the States, which is where it should be.

I see nothing in the way the Commission is structured or the other elements of this bill to effect day-to-day management of law enforcement operations. In fact, I think this bill comes closer than many others to giving the control back to the States.

A point that needs to be considered is that there is, right now, today, de facto regulation by the Federal Government in terms of the control that the FBI Director exercises over NCIC. At this point, States have no control over the National Crime Information Center and those criminal history records which they put into the system.

The States own that data. Yet, the NCIC has only an advisory board consisting of State and local officials to help it make decisions. I am saying that the fact is that de facto regulation now exists. You cannot argue that this bill does anything worse. If anything, the Commission really produces the influence that the States should have over the control of this information.

Senator TUNNEY. You addressed yourself to section 208, as did the chief. The chief indicates that he feels that the requirements for the sealing and purging of certain arrest record information in the event of nonprosecution are highly unrealistic.

The decision not to prosecute may have been based on a tangential matter, such as the exclusion of essential evidence or the decision of a key witness not to testify, as often happens in sex offense cases, or a public attitude opposed to full enforcement of certain laws.

He feels that this requirement should either be eliminated or significantly changed. As I understood your testimony, you feel that section 208 is unduly restrictive?

Mr. WORMELI. Yes, sir. I agree with Chief Pomerance on that point. I think particularly the parts which talk about sealing and purging due to lack of prosecution are overly restrictive.

I can think back to Washington, D.C., just a couple of years ago when there were not enough judges to prosecute the cases. The prosecutors were only filing about half of the arrests that came to their attention.

There were a lot of good cases which probably would have resulted in convictions had there been enough judges and enough prosecutorial time to deal with it. Under these provisions, those cases would have been lost to the police for their further use in investigative ways.

I think it is important to remember that the abuses of arrest records have largely not been that of the police. If we are going to ask them to do a job, as the chief pointed out, they should have that tool.

Senator TUNNEY. Are you suggesting that section 208 be taken out in its entirety?

Mr. WORMELI. No, sir. The sealing and purging of a person free from jurisdiction for 7 years is an important change in our whole concept of dealing with criminal history information. The time is long overdue when we recognize that after some period of time—and 7 years is long enough—the stigma imposed by a criminal history should be removed from an individual.

Senator THURMOND. I received a telephone call today from Mr. J. P. Strom, chief of the South Carolina Law Enforcement Division, and he indicated he is opposed to this bill.

I think his feeling is expressed on page three of the statement by Rocky Pomerance, president of the International Association of Chiefs of Police.

> Essentially, we believe that S. 2008 unnecessarily imposes upon State and local agencies standards dictated by the Federal Government, which would grant the Commission the ability to control the day-to-day details of State and local criminal justice administration.

I felt I should make that statement for the record in order to express Chief Strom's opinion on this legislation. He feels it is an intrusion by the Federal Government to enter the field as he feels S. 2008 does.

Thank you very much.

Senator TUNNEY. Thank you, Senator Thurmond.

Chief Pomerance also evaluated section 308 of the bill and he found it lacking. He said that he feels that by "allowing an aggrieved person to bring civil action for violation of the act or regulations promulgated pursuant to it", that it will seriously impede the legitimate activities of law enforcement officials.

He talked about a "chilling effect upon law enforcement efforts in any situation which might arguably violate the act or rules and regulations."

Do you care to address that point?

Mr. WORMELI. I would have to take the position that the chill factor is a little bit overestimated in this case. I can only point to the many law enforcement officials throughout this Nation who participated in the Project SEARCH deliberations which led to the introduction of Senator Ervin's bill a year ago, and which led to the publication of the standards and procedures for security and privacy in Criminal Justice Information Systems in 1970.

Those law enforcement officials were of the opinion as far back as 1970 that civil remedies were a necessary part of any legislation which might come out in this field. I think the most progressive law enforcement officials, upon careful reading of what I hope will be the final version of this bill, will agree that such a remedy is necessary.

The bill more appropriately centers on what is a proper response to charges and whether or not the proper conduct of activities and good intent is a sufficient cause for explaining what happened.

I think at that level, there is still room for debate. What amounts to proper conduct is knowledge of the relations promulgated under the Act and the good faith and attempt to carry them out.

If so, can that be demonstrated? That is a difficult issue and not being a lawyer, I am not sure how to write those words.

Senator TUNNEY. Have you had any personal contact with any jurisdictions in which a similar provision in the law exists?

Mr. WORMELI. Yes, sir. There are several States right now that have civil remedies allowable under their law. I believe the new Oregon law follows much of what you have in your bill, including that section.

There are certainly a number of sanctions that have been imposed throughout the country in the States that have passed laws like this already, including Massachusetts and Oregon.

Senator TUNNEY. Has it led to a chilling effect, to your knowledge?

Mr. WORMELI. Not to my knowledge, Senator. In fact, to the contrary. I find that most people operating under the laws that have been passed, which are more stringent than S. 2008, find it quite livable.

Senator TUNNEY. Do they find it helpful because they are not then under pressure to divulge this information to persons who should not have it, like reporters or credit agencies or prospective employers? If there were a law which said that it was, in effect, a violation of the statute to make such information available, they would have protection against that peer pressure because they could say, "Look, I am not going to violate the law. You cannot get me to do that."

Now they do not have that protection.

Mr. WORMELI. California, for example, requires the State division of identification to give out criminal records based on submission of fingerprints for a wide variety of licensing applications like barbers' licenses. The State identification bureau does so because the Governor or the attorney general tells them to.

In my view, whether they would say this or not, I cannot be sure, but in my view, they consider it more of a nuisance. The purpose of this data is to help criminal justice. The fact that every licensing agency or other entity in the State also wants to check out their employees is a secondary benefit from these systems, not a primary purpose for these systems.

Most law enforcement officials would prefer to have the statute spell out, either at the Federal or State level, exactly who should be given access to these files and for what reasons.

Senator TUNNEY. The thing that I think is going to trouble many Senators—and certainly, when I first got involved in this legislation, troubled me—was the question which you have already addressed, but which was also raised by Senator Thurmond, and that is: Does this represent an intrusion of the Federal Government into local law enforcement policy and activities?

The point which you have addressed very articulately is that already, through the NCIC, the FBI has a substantial intrusion into the telecommunications of the various States.

I think in many instances it has been most beneficial for society. The fact that a police officer in the field making an arrest was able to get an almost instantaneous check of the record of a person, which sometimes demonstrates that the man who is being stopped has a felony record or is a wanted criminal, has been very beneficial.

But the problem is establishing standards to control the system, to make sure that you are not creating a monster; a system which, if under proper regulation, supervision, and direction, would never create difficulties.

Where there is irresponsible direction or supervision, significant and widespread violations of individual liberty could result. As one who has done so much work in this area, is so familiar with the computer systems and with the basic law enforcement problems that underlie these computer data systems, could you elaborate a little more on what you consider the present intrusion to be, and what would be possible if we do not get some legislation controlling that telecommunications capability which the FBI is now developing?

Mr. Wormeli. There is an important first step that I think the subcommittee will have to consider and that is to try to break this problem down into some smaller parts.

The National Crime Information Center provides a necessary service to all of law enforcement in its collection of records on wanted persons and stolen property and stolen vehicles. Those subsystems, if you will, are already in operation. They have been in operation since 1966, and they are crucial—crucial—to law enforcement.

No one expressed any concern on any side of the issue about the security and privacy of those records. It was not until we began to consider inserting an additional file or a new system into NCIC, one that would contain the criminal history of persons, presumably forever, that this became a problem.

Now we are faced with the development of a new system whose size could be much greater than all of the existing systems put together and which would contain data that many people find potentially damaging.

The wanted persons-stolen property-stolen vehicle fields need not be discussed. The telecommunications is nothing more than finding a way for the police department to get from wherever it is into the national file. And certainly, NCIC should continue to provide access by everyone to these existing files. The criminal history file is a different kind of an animal.

There is already the development of policy on the part of NCIC and the FBI and, as expressed in the Department of Justice regulations and in NCIC's own policy which dictates how the criminal history file will operate. The States have only the voice of an advisory policy board which advises the Director of the FBI on uses to be made of that file and on the contents of that file. The staff work for that Commission is done by the FBI. I would suggest that at the present time, the FBI does, indeed, determine the nature of the interstate criminal history exchange system.

Whether you call that intrusion, it seems to me that it is a fact that they have policy control. I think many people, upon reading this bill

for the first time, may not be aware of the background of why that Commission was first proposed.

It was proposed precisely to give the States more of a direct policy voice in the operation of a system to exchange interstate data. Initially, it was proposed by the States in 1970. It has been endorsed by Project SEARCH on repeated occasions since then, and by many other groups.

The important fact is that the majority of the members of the Commission, 7 of the 13, are State officials. The States would have the policy voice over systems like the criminal history subsystem of NCIC, so that what they can mutually work out through that Commission would be satisfactory to all the States.

I am not criticizing what the Bureau has done. Nor am I criticizing any of the other Federal agencies for doing what they felt they had to do. But, I think it is critical that the Congress speak to this issue.

It is a Constitutional issue. It is an issue of State-Federal relationships. It is bound up in the new federalism and the basic concept of how grant programs are working. It cannot be resolved by executive fiat.

Senator TUNNEY. I want to thank you very much for your excellent testimony. It is a real privilege to talk to you. I can ask you many more questions, but I have been informed that an amendment is up to my bill and I have to go over and defend against an "intrusion".

[The prepared statement of Mr. Wormeli follows:]

PREPARED STATEMENT OF PAUL K. WORMELI, VICE PRESIDENT, PUBLIC SYSTEMS, INC.

Mr. Chairman and members of the Subcommittee, I wish to thank you for your invitation to appear before you to comment on S. 2008. My remarks will be based on my experiences in a number of national projects dealing directly with this issue. The effective and proper use of criminal history information has occupied a great deal of my time during the past six years.

First, let me say that I believe S. 2008 to be a distinctive step forward in the legislative deliberations regarding criminal history information. This bill is, as the Chairman has stated, a much clearer and precise coverage of the issues than has been afforded by earlier proposed legislation. I strongly believe that the provisions of S. 2008 provide the basic protections of individual privacy while at the same time preserving the right of law enforcement and criminal justice agencies to obtain the data necessary for their effective operations.

A delicate balance between individual rights of privacy and the needs of criminal justice agencies is difficult to maintain. However, defining such a balance is an absolute requirement if progress is to be made in improving the administration of criminal justice. As members of the Subcommittee know, the criminal justice community instigated the first efforts to provide for the protection of individual rights of privacy in computerized criminal history systems while attempting to clarify the legitimate needs of criminal justice agencies for data on the histories of criminal offenders. The work of Project SEARCH over the last six years has been the basis for various attempts at legislation. Statutes have been enacted in many states which reflect the initial principles proposed by Project SEARCH in 1970.

It is critically important that any legislative action at the federal level reflect the importance of providing information to those agencies and individuals charged with carrying out criminal justice functions. Criminal offender record information and the statistics derived therefrom are the critical thread that links the various parts of the criminal justice system. To begin to deal with improving the administration of justice, it is imperative that we begin to understand the flow of individuals through the criminal justice system, and that we provide the data needed by law enforcement officers and other officials in a timely and accurate fashion. There is no other way to properly plan for the improvement of the system than by examining the performance of the system in terms of its common element; namely, the persons to whom the criminal justice sanction is being applied.

I believe that the lack of legislative action to date has been an impediment to progress in this field. As Senator Tunney pointed out in introducing this bill, both the House and Senate have been considering these issues for the last four years. The many complex issues, both Constitutional and technical, prohibit the finding of easy solutions. However, the time to find the solution is now upon us. Progress in the development of effective and accurate criminal history information systems has been seriously impaired because of the lack of federal action in the development of statutory standards for the control over these systems. Many state and local governments have been unwilling to move forward to provide this necessary data to criminal justice agencies because of the lack of agreement at the federal level as to what standards will be imposed. Without an end to this confusion, governmental agencies throughout the country will not commit themselves to providing the tools required by law enforcement. I believe that most people in the criminal justice community are now at the point where they would be relieved by any action by the Congress, regardless of the nature of that action.

As Senator Tunney mentioned in his introduction of the bill, there are an increasing number of court cases that are attempting to deal with the storage and dissemination of criminal history record information. If the Congress fails to act to establish the national standards by law, interpretation decisions will be made independently by a variety of individual courts in dealing with these cases. Some decisions have already been made which provide conflicting approaches to the use and dissemination of criminal history information. In view of the potential expansion of computerized systems, a statutory basis for controlling these systems is required now.

As a general comment on S. 2008, I find myself in complete agreement with most of the provisions of the bill. Recognizing that many of these issues are complex, I believe that the bill strikes a reasonable balance between the points of view which have been expressed in past hearings and by a variety of interest groups. I believe that most criminal justice officials will find this bill easy to live with. As far as I can tell, the provisions in the bill are consistent with Project SEARCH recommendations for legislation in this area. The endorsement of such a national body, reflecting the views of senior criminal justice officials in each state should be far more relevant than whatever remarks I can add.

I would now like to comment on some of the specific provisions. With respect to the sections of the bill dealing with the use and dissemination of these records, I would urge the Subcommittee to keep in mind that the abuses which have occurred in the use of criminal history information have been primarily related to uses by organizations and individuals not performing criminal justice duties. Most of the court cases which have been cited in support of the need for this legislation deal with the use (or abuse) of criminal history information for employment purposes. It is my personal opinion that most criminal justice agency officials consider the transmission of criminal history information to employers to be more of a nuisance than a part of their normal function. While there are legitimate arguments for providing relevant criminal history information to employers under carefully defined circumstances, the primary purpose of collecting this data is to help criminal justice agencies carry out their statutory functions. I believe that the provisions in S. 2008 provide a basis for the legitimate collection and dissemination of both arrest and conviction information to criminal justice agencies. The bill also provides adequate controls on secondary dissemination and the use of criminal history information for other non-criminal justice purposes.

A major concern to the criminal justice community as well as the public and individuals involved is the security and accuracy of the information. Much of the fear associated with the use of these files would be eliminated if the agencies keeping the records could assure everyone that the records are complete and accurate, which is certainly not the case with the existing manual systems.

There are two key provisions in Section 207 of the bill, dealing with the security and accuracy of criminal justice information, which should be preserved and made law regardless of what happens to any of the other provisions of the bill. First, the bill provides for a clear policy that dispositions shall be reported and recorded along with arrest record information. The lack of disposition reporting is clearly the major impediment to the success of these systems. The second key provision is that any information which becomes a part of a record or file should be supported by verification of the identity of the individual. It may be advisable, given the present state of the technology, to add to this provision the necessity for fingerprints to be used as a basis for the verification of identity.

For the most part, the provisions on sealing and purging are consistent with the prior proposals of criminal justice agencies themselves. The requirement for purging if no prosecution is undertaken may not necessarily be the most effective

way to operate the system. Since prosecutions are frequently not begun because of the lack of staff or for other reasons not relative to the case, it may be desirable to provide for a longer period in which the arrest data could be maintained for use by criminal justice agencies. In fact, I would go farther and state that the provisions of Section 208 which call for the sealing or purging of arrest record information are, in my opinion, overly restrictive. There are many legitimate instances in which law enforcement agencies need access to a record of arrest, regardless of whether or not the prosecutor has chosen to file. In view of the fact that abuses of this data have not been attributable to the law enforcement agencies as much as to non-criminal justice agencies, and because of the influences outside the control of the law enforcement agencies regarding potential prosecution, it would appear to me that the controls over *dissemination* of arrest information would suffice to protect individual privacy.

S. 2008 introduces a change from prior positions taken on the availability of computerized intelligence information. I believe that the index which permits interagency exchange of the existence of records maintained for intelligence purposes should also contain that common public record information which is verified and supported by other documentation. The discipline required by the bill for the maintenance of intelligence information systems should lead to an improved quality in the intelligence information available to criminal justice agencies. Public record data, such as ownership of corporations and other public documents, provides a common basis for investigation of organized crime individuals which should be shared by the agencies investigating a particular individual's activities. A legitimate concern of such agencies would be unnecessarily impeded by the restriction on exclusion of public record information.

I would now like to turn to several issues which are not contained in S. 2008, and urge your consideration of these additional matters.

One of the issues of great concern to state and local governments is the authority and the limits on activity to be granted to the Federal Bureau of Investigation in its operation of the National Crime Information Center. Criminal justice officials throughout the nation rely on many of the services of the National Crime Information Center. There has never been a clear definition of the services which the FBI should provide to state and local governments. For the last five years, substantial debate has ranged throughout the Executive Branch of the federal government, involving a great deal of time and causing substantial confusion in the minds of the criminal justice officials who seek to work out agreements between the FBI and their own governments as to responsibilities for the collection, preservation, and dissemination of criminal history information. Policy legislation on this matter appears to be the only way to resolve the confusion. The debate over whether or not the FBI should provide message-switching services, as opposed to a consortium of states created to provide such a national service, appears to be irresolvable in the Executive Branch of government. Through a succession of Attorneys General different points of view have been aired, without any final resolution.

I strongly believe that the only way to solve this problem and eliminate the confusion is for the Congress to specifically proscribe the services which the FBI should provide to local agencies. I believe that the issues are not irresolvable, and that this current bill is a logical place to delimit the functions of the FBI with respect to criminal history information as well as other information exchange and telecommunication services. The cost of delaying a final decision on this matter, even by attributing powers to the Commission proposed in Title 3 to make such a decision, is enormous. Thousands of man-hours have been spent in discussing this issue and in proposing various positions. It is time for a resolution, and the Congress is the proper body to reach a decision.

Another issue of grave concern to state and local officials has to do with the controversial subject of whether dedicated or shared computers should be used to store and disseminate criminal history information. As members of the Subcommittee know, the Department of Justice has issued regulations under the authority of Section 524 of the Omnibus Crime Control and Safe Streets Act for the protection of individual privacy and the security of systems. These regulations call for the use of only dedicated systems for the storage and dissemination of criminal history information. Those of us who have been actively involved in the criminal justice field for some time support the concept of dedicated systems. Particularly at the state level, there are enough functions and purposes to be served by the use of the computer which require a highly responsive system that justify the development of a dedicated computer. Project SEARCH, as far back as 1970, endorsed the general principle of dedicated computer systems for the storage of criminal history information. I personally endorse dedicated systems, particularly

at the state level where repositories of criminal history information will be developed. In my mind, such systems are justified primarily on the basis of giving law enforcement and criminal justice agencies the response they require to perform their functions. No serious technologist would argue that provision of separate computer systems for criminal justice will not increase costs. I believe that the responsiveness and need for data by criminal justice agencies outweighs the economic arguments against dedicating these systems. At the same time, however, I do not believe that the concern over privacy and security is a sound basis for insisting upon dedication.

The Department of Justice regulations should have defined the levels of security to be provided by any system, regardless of whether it is shared or not, rather than to impose a particular solution which is highly debatable. Dedication of a system in its own right does not guarantee privacy nor security. It is an intuitive attempt to promote improved privacy and security. While LEAA should promote the development of responsive criminal justice information systems, I do not believe that the federal government should be in the position of dictating specific solutions to state and local governments when the policy provisions have not been well articulated. For your consideration, I would propose that this bill either repeal that particular section of the Department of Justice regulations which deals with dedication, or considerably narrow its scope to limit the coverage to repositories developed at the state level for criminal history information.

The remaining parts of the Department of Justice regulations are sound first steps in improving the accuracy and completeness of criminal history information systems and in controlling the uses of such systems. It would seem appropriate to complete this bill with a reference to these regulations as a first attempt, on which the Commission mentioned in Title 3 can build additional regulations. Some such reference would further integrate the development of improved procedures in this field.

Senator TUNNEY. The subcommittee is now going to adjourn until tomorrow, when we will reconvene at 8:30. Initially, we had said 9:30, but we are going to run into problems. We will reconvene at 8:30 so we can be assured of hearing the Deputy Attorney General and his testimony.

I would ask the staff to inform everyone.

[Whereupon, at 12:15 p.m., the hearing was adjourned, to reconvene at 8:30 a.m. on Wednesday, July 16, 1975.]

56-833—75——14

# CRIMINAL JUSTICE INFORMATION AND PROTECTION OF PRIVACY ACT OF 1975

WEDNESDAY, JULY 16, 1975

U.S. SENATE,
SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS
OF THE COMMITTEE ON THE JUDICIARY,
*Washington, D.C.*

The subcommittee met, pursuant to recess, at 8:40 a.m., in room 2228, Dirksen Office Building, Senator John V. Tunney (chairman of the subcommittee), presiding.

Present: Senators Tunney, Hruska and Thurmond.

Also present: Jane L. Frank, chief counsel, Douglass Lea, majority counsel, J.C. Argetsinger, minority counsel.

Senator TUNNEY. Today is the second and concluding day of this series of wrap-up hearings on criminal justice information bills. As I indicated yesterday, these investigations have continued over several years, and the record is very forceful in presenting the need for such legislation. We are now trying to put the finishing touches on this legislation by receiving final comments from interested parties. The record of these hearings will remain open for written statements for a period of 2 weeks after today.

Our first witness today is Harold R. Tyler, Jr., the Deputy Attorney General of the United States. During the past year the Justice Department and the Constitutional Rights Subcommittee have moved steadily closer to each other on both the philosophy and substance of this issue. I hope that this spirit of cooperation can continue as the debate focuses on the details of the legislation and that we will be able to accommodate the Justice Department's desire to have specific criminal justice legislation before September 27, 1975, the effective date of the Privacy Act of 1974.

Mr. Tyler, I would like to say how grateful I am for your appearance here today. It certainly does help the committee to have the Deputy Attorney General present speaking for the Department.

## TESTIMONY OF HAROLD R. TYLER, JR., DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE; ACCOMPANIED BY MARY LAWTON, U.S. DEPARTMENT OF JUSTICE

Mr. TYLER. I thank you, Mr. Chairman.

As the subcommittee knows, Miss Mary Lawton of the Department is with me here this morning.

In addition to our prepared testimony I would like to note that we would offer to the subcommittee a publication of the LEAA compendium of State laws governing privacy and security of criminal justice

information. This is a recent publication which I think brings us up to date on the current conditions of State laws in this sensitive and difficult area. And I will have it available for the subcommittee and the staff as they desire.

Senator TUNNEY. Thank you very much.

Senator HRUSKA. Mr. Tyler, are they available in larger numbers?

Mr. TYLER. Yes.

Senator HRUSKA. We may want copies for members of the Judiciary Committee.

Would that be in order, Mr. Chairman?

Senator TUNNEY. It certainly would be in order, Senator.

Mr. TYLER. We will see to it that a number of copies come over.

Although we are not always as timely as we would like to be and ought to be, Mr. Chairman, I believe that we did have copies of our testimony here at least a day in advance. Nevertheless, I will conform to your wishes on the matter.

Would you like me to summarize my testimony?

Senator TUNNEY. I think that that would be appropriate, first of all, so that Senator Hruska and I can ask some questions, and second, because we have a small matter on the floor which comes up at 10 o'clock. We will have to conclude by 10, so it would be appreciated if you could summarize your testimony.

Mr. TYLER. All right.

I will now proceed.

As the subcommittee knows, and as the chairman briefly stated this morning, there has been a considerable amount of work in both Houses of Congress and in the Department of Justice for approximately the last 4 years in this area.

Speaking for the Department, it appears that they began drafting legislation on the exchange of criminal justice information in 1971. In November of 1974 the Department submitted a virtually complete revision of its views as to a criminal justice privacy bill to the Congress. This really is the same proposal or bill which you, Mr. Chairman, introduced on April 14 of this year, as S. 1428.

We are basically still of the view that the proper balance is substantially set forth in S. 1428. And we support its enactment.

Conversely, we have considerable difficulties with S. 2008, at least in its present form, partly because of drafting problems which we perceive and, more fundamentally, because we have certain conceptual and substantive disagreements with that proposal as it now reads.

Of course, as we have all known in the past years, and as we have discussed privately and publicly, we are in a difficult posture in this kind of subject matter, because we are involved in a tension between two important rights: The right of the public to know and to see to it that law enforcement activities go forward, and on the other hand, the individual right to reasonable privacy, that is, privacy where there is no public right to intrude.

The Congress and others have been concerned about usages of criminal justice information which is inaccurate or totally unnecessary for the law enforcement purposes for which it is asserted.

On the other hand, the police and criminal justice agencies, which are under great burdens and suffering from past inefficiencies, cannot function unless there is prompt, accurate dissemination of criminal

justice information by which we mean all kinds of categories like criminal intelligence, rap sheet information, fingerprint identifications, and other forms of identification and licensing information.

Now, of course, law enforcement in our country is not the sole province of the U.S. Government. Indeed, it is basically a matter of State and local concern, with Federal law enforcement jurisdiction carefully and tightly circumscribed. This means, among other things, that as we discuss this difficult subject matter this morning, we must recognize that important as we may think the Federal role is, it is by no means statistically and otherwise as vast in its complexity as are the State and local law enforcement agency interests in this area. Indeed, as we know, the usages of computer technology have gone forward very strongly in a number of the States.

The States have recognized, or at least a number of the larger States have recognized, the capability for the exchange of information by computer technology. And this has reinforced the collaboration and interdependence of various State and local law enforcement agencies in the United States.

In recognition of this matter, among others, both the bills heretofore identified extend not only to Federal agencies but, of course, most importantly to State and local agencies which operate with Federal funds, exchange information interstate, or exchange information with Federal agencies.

S. 1428 recognizes the primacy of State and local government in the criminal justice area by carefully avoiding imposition of strict and overly comprehensive Federal control on State agencies. In our view S. 2008, however, which purports to set up a Federal commission to oversee administration and enforcement of the provisions of that bill, particularly with power to issue binding regulations and interpretations, is quite a different matter.

While that bill encourages the creation of State agencies to perform the functions within a State, it also seems to us that the bill provides that those agencies would be regulated by federally established guidelines. In our view this goes too far and upsets the proper balance of Federal-State relationships, at least within the area of law enforcement.

Now, as stated, we are continually challenged in our drafting work here—when I say we, I mean this subcommittee and the Department and everybody else that is interested—in striking the proper balance between the protection of the public through law enforcement and the protection of individual privacy interests where they are paramount. In many senses, you could say that neither of the bills in its terminology, nor in its specific terms, of course, attempts to do this. Rather, each bill really tries to make sure that politically responsible officials at both the Federal and State levels decide on a case-by-case basis, and as new problems and new concepts arise, whether it is more important that a potential employer, for example, knows of a past criminal record, or that that particular prospective employee's privacy be protected.

S. 2008, however, seems to circumscribe this decisionmaking by foreclosing access to certain records and providing for the sealing or destruction of other records.

Furthermore, it permits decisions on access to be made only by the legislature at both Federal and State levels.

Conversely, as you know, S. 1428 permits a decision on the availability of records and information to be made by the Chief Executive as well as the legislature at both Federal and State levels.

This type of decisionmaking would extend not just to criminal justice records of a restricted type, but to all types of criminal justice records so long as the decision is made publicly and it is absolutely specified as to what types of records are being dealth with and made available.

Now, let me turn a little bit more specifically, if I may, to some of the fundamental concepts as we see them in these two important drafting efforts. And in the process, if you would permit, I would like to explain in a little more detail our objections to S. 2008 as it now stands.

As I have already said, the basic difference in approach between the two bills is that S. 2008 attempts comprehensive regulation of the subject, that is, regulation of criminal justice information. It attempts to forbid uses not specifically authorized in that bill. On the other hand, S. 1428 takes a different approach. It seeks to lay out firm goals, to provide minimum standards, to focus on identifiable problems as we know them now, thereby leaving room for further refinements as experience and expertise are developed.

Parenthetically, let me say that I note in every one of our discussions internally—and the same was true on Monday morning before Congressman Edwards' subcommittee—that when we begin to deal with the various fact problems that can arise in this area, it is almost as if we were seeking to top one another by our stories as to what could happen.

I mention this because it seems to us—and this we think is important—that as much as we believe we know now about the kinds of problems that will arise in this area, even the case law in the courts indicate that there are myriad situations which it would be unrealistic for the subcommittee or the Congress to anticipate specifically by black letter drafting now.

I hardly need to add that although we think we know a good deal about computer technology in 1975, as an unknowledgeable lawyer, I still would offer the sincere suggestion that we may not know all we ought to know about computer technology quite yet either.

Thus, for those two broad reasons we believe that the thrust of having minimum standards and goals—without attempting to regulate specifically every contemplated privacy and criminal justice problem that mankind could think of in July, say, of this year, that that is the better approach. Set the goals, put the minimum standards in, allow the Commission as they go along to take up new factual developments and new problems expertly and continue to refine the process in the ensuing years.

In short, Mr. Chairman, and members of the subcommittee, we believe it would be premature to apply a preclusive approach such as that in S. 2008 to the thousands—and there are literally thousands, as you know—of Federal, State, and local criminal justice agencies which would be covered by legislation of this type. In our view it is far more sensible to address the specific problems which will be identified and which have already been identified through a mechanism

such as the Commission proposed in S. 1428 to take into account new developments and the myriad different fact patterns as they arise in the future.

Of course, in making this point we do not ignore that both bills recognize the interdependent, interconnected role of Federal, State, and local agencies. I mention that point, and it is an important point. But I would also like to point out our concern that the two bills have a different approach here as well.

Very briefly, S. 1428 would apply uniform Federal standards to interstate exchanges of information, and exchanges between Federal and State agencies.

At the same time, and in the process, however, we think that bill continues to recognize as it should the primacy of State laws within State boundaries—so long, of course, as the State law in that particular State meets the minimum Federal standards.

S. 2008 provides that State law will govern all maintenance, dissemination, and use of information within the State insofar as it imposes stricter standards than Federal law.

That bill suggests that such State laws will regulate not only State and local agencies within the State, but, in addition, Federal agencies located within the State boundaries; such as a local IRS office engaged in criminal tax intelligence work, or perhaps even a local office of the FBI, and so on.

It would be read also to impose restrictions on information found within that State, even though that information originated in an agency of a different State, or in a Federal agency such as the FBI, the IRS, the DEA, or whatever.

It might even be interpreted to apply to information being exchanged by two States but passing through a third State which happened to have stricter laws. There is a considerable question whether States, even with the permission of Congress, can impose standards on the use or dissemination by Federal courts of information acquired, maintained or used by these courts, simply because of their physical location within a particular State.

In short, Mr. Chairman, we are concerned here about possible serious difficult issues of Federal supremacy, separation of powers, and the like. Beyond that, I do not think we have to stress that the practical effect of such provisions is confusing, to say the least, in their application.

Turning to another subject, let me as swiftly as possible note that both bills extend, of course, to all major aspects of criminal justice information, that is to say, criminal history, investigative information, criminal intelligence, correctional information, court statistical information, and so on. And both bills address, at least in some respects, the collection, retention, use, and dissemination of such information. But the bills do differ in the degree of specificity with which they purport to regulate this information, and in the number and types of subcategories into which they divide the information.

We think that the differences in definitions make it difficult, quite frankly, to compare the two bills as precisely as we know the subcommittee would like to, and as we would like to.

Let me illustrate this by pointing out that S. 1428, for example, speaks of what is called arrest record information, which has no disposition attached, and criminal record information, which means that a disposition is attached.

S. 1428 defines disposition with some care and particularity. That bill uses criminal justice information to encompass arrest and criminal record information, correctional information, intelligence, and the like.

Turning to S. 2008, however, that bill refers to arrest record information, nonconviction information, and criminal history information. It uses criminal justice information to mean those terms mentioned above plus correctional and release information. But it does not have any general term to encompass all types of information.

Turning back to S. 1428, that bill defines disposition to include a variety of procedures for terminating a case, including even pretrial diversion, whereas in comparison, S. 2008 uses the same term to mean only a dropping of charges, or a conviction.

Now, in addition to such definitional distinctions and problems, there appears to be a difficulty in treatment of intelligence information, as the two bills are presently cast. S. 1428 in general terms provides for confining intelligence collection to official purposes, limiting access on a need-to-know basis, and requiring an accounting of exchanges with other agencies.

On the other hand, S. 2008 attempts by its terms to define standards for maintenance of intelligence. Maintenance is not defined. It appears that it would be authorized only "if grounds exist connecting such individual with known or suspected criminal activity and if the information is pertinent to such criminal activity." Information could be sent to another agency only to confirm information in that agency's possession or for investigative purposes if the other agency can "point to specific and articulable facts which taken together with rational inferences from those facts warrant the conclusion that the individual has committed or is about to commit a criminal act."

Mr. Chairman, we have considerable difficulty with these standards because they are vague, and because they seem to have been borrowed from some case law. The standards are unexceptional in the contest in which that case law was decided, but they would really seem to be very difficult—almost impossible—to engraft here. As you see from my printed text, we are talking here about the case of *Terry* v. *Ohio*, which of course as we all know deals with stopping and frisking a suspect by a cop on the beat. That is an important area. And I don't deny it. But what I am trying to say here is that the standard which the Supreme Court says is applicable to a stop and frisk situation on the street of a city or a town is quite a different matter from trying to set up a standard to determine what information can be volunteered, for example, by one agency to the FBI in connection with some serious and complicated felony, or to the Secret Service, as the printed text suggests, in connection with a threat of assassination of the President or some other high Government official.

As S. 2008 is set forth, dissemination to another agency is authorized only to confirm information that agency already has, or when the so-called articulable fact standard is met. We really worry about this, for this simple reason, and the reason has to do with the nature of

intelligence. As we all know, intelligence really is gathered by little bits and pieces of information which flow from various people, various sources, both official and public, and sometimes and informer. Sometimes a scrap of information, as innocent as the report that somebody has entered a telephone booth, proves to be most important.

The mosaic of intelligence has to be put together piece by piece, bit by bit, more often and not. And there can be no more difficult task for a police agency.

Senator HRUSKA. Would you yield on that point for a question or two, Mr. Tyler?

Mr. TYLER. I certainly would, sir.

Senator HRUSKA. At a later point in the bill there are penalties against the improper disclosure of information, and improper transmission from one agency to another. Now, with this standard to which you refer, namely, that information from community B can be sent to community A only if community A can point to specific and articulable facts which taken together, with rational inferences from those facts, warrant the conclusion that the individual has committed or is about to commit a criminal act.

Who in that sequence will be responsible for judging whether or not there is the proper relevance and the proper foundation for making the request—will it be community A, or will it be community B—in an effort to avoid penalties if there is an improper transmission of the information?

I read that language from the top of page 10 of your statement.

Mr. TYLER. It would appear that the agency which has this information in its possession, will have to look to specific and articulable facts, and so on. That in itself seems to me very confusing conceptually and practicably.

Of course, whatever agency has the responsibility, it is an almost impossible task because that agency's officers will only have a few bits and pieces of information, and yet they will know as proper, prudent police officers that perhaps this piece of information might be very helpful to somebody else who has more pieces of the mosaic. So that on two counts this matter is very difficult: the count you mentioned—who is it that really is going to make the determination which we say is not clear, and second, even on one that is clear, how is he going to do it, because it is just impossible in the practical everyday work of criminal intelligence gathering for one agency, or even several, to point to specific articulable facts, and so on, from which the rational inferences can be drawn.

Senator HRUSKA. The law enforcement agency of whom a request is made will have to make that decision, and it will have to have all the facts in the file of the requesting agency, isn't that true?

Mr. TYLER. That seems to be a fact.

Senator HRUSKA. And that would be quite an undertaking, would it not?

Mr. TYLER. Right.

Senator HRUSKA. It would probably clog the line.

Mr. TYLER. You would have to shear back, so that the standard could be met. In other words, if I were agency B, and I requested information of you as agency A, you would have to say to me, "Well, wait a minute, you are going to have to tell me all you know, so that I can make a determination whether the standard is met——"

Senator HRUSKA. And whether my reply to you will be legal or not?

Mr. TYLER. Right. I am sure the draftsman had the proper concern here—they wanted to make sure if possible that there wouldn't be just a willy-nilly exchange of information which truly was not serious criminal intelligence. But I think in their concern they have set up two rather confusing and unworkable concepts for trying to meet that type of problem.

Senator HRUSKA. I am not sure what the objective is, but I conjecture that the objective there was to prevent just plain nosiness and fishing expeditions that would be aggravating to an ordinary citizen who didn't do anything, and yet whose affairs could be pried into and information about him could be batted back and forth on the computer system.

Mr. TYLER. Right.

Senator HRUSKA. But taking into consideration the legitimate needs of the law enforcement community, this provision appears to raise some very difficult practical problems.

Let me move to another practical problem which might arise in that same context. A little bit later on you refer to an unwarranted extension of the exclusionary rule of evidence. Would there be the possibility of that if some of the information that is transmitted in response to a request from one law enforcement agency to another did not meet the test of the language which I read from the top of page 10 a little bit ago, there could be a conceivable challenge against the legality of that evidence, and therefore the exclusion of it, and therefore the illegality and the impropriety of the conviction if such is obtained in the trial?

Mr. TYLER. We believe that the answer to that essentially is yes. And that, of course, is a cause for great concern, particularly now, in that the Supreme Court is in the process of reconsidering the exclusionary rule. But more than that, we think that whatever the courts may be doing, it is very difficult to engraft an additional responsibility on law enforcement people to be concerned in this difficult area with making hard and almost impossible choices, only to face a situation where a court would be required to throw out a whole line of evidence just because one piece in the interchange as contemplated here was not correct.

Senator HRUSKA. And that long line would be tainted and therefore would be improper.

Mr. TYLER. Right.

Now, I am sure again the draftsmen were concerned with the possibility, that occasionally somebody could, if uncontrolled, go too far. But this goes back to the point which really permeates, I believe, all of our testimony here this morning. We think that the way to get at these possible problems is not to have a bill which purports to be restricted by its terms. We believe, as I have said, that the better approach is to set minimum standards, have a commission, and employ a procedure where, as problems develop in the future and we know more about them, then we can strike the proper balance on each occasion without all-embracing black letter rules, exclusionary rules, and penalties for different kinds of decisions which should not have to be made by law enforcement people trying to do the work on a daily basis.

Now we, of course, have to recognize, and I believe we do recognize, that standards for intelligence collection and dissemination have to be considered and established. This subcommittee knows, for example, that the Department of Justice is now attempting to formulate guidelines for the FBI with respect to intelligence collection, dissemination, and the like. I have to say that the more we got into the issue this spring and summer, the more complex the problems appeared.

And therefore, even for the FBI, with its comparably limited jurisdiction, we are now beginning to recognize that it will be some time before we can adequately set up guidelines and have them considered by all interested parties. If it is going to be difficult for us with the FBI, think of what this is going to amount to if we have a bill that tries to set standards for all of the Federal agencies, the State agencies, and the local agencies, that would be recognized by these bills under discussion today. Therefore, we think it impracticable and premature to attempt to formulate such standards.

We believe that the wiser course is to allow all these myriad agencies to formulate their own guidelines, at least at first, subject, of course, to study and recommendation for revisions, et cetera, by the proposed commission, as it develops experience and know-how in the next years.

This, as you know, is the approach of S. 1428.

Now, we have considerable difficulty, as we mention in our prepared remarks here today, with the investigative information area as it is dealt with in S. 2008. That bill, as you know, would require that investigative information could not be maintained beyond the expiration of the statute of limitations for the particular offense in question, or the sealing or purging of criminal history information relating to that particular offense.

As we illustrate, if a marginal securities fraud case in New York, for example, is not referred for prosecution, both the criminal history record and any investigative files would have to be sealed or destroyed. Any subsequent investigation of a similar case, perhaps involving some of the same people, would have to begin from scratch. Moreover, investigative files would have to be sealed or destroyed upon the running of the statute of limitations, regardless of their relevance to later cases.

We are not at all convinced that this is really the intent of S. 2008. And yet its literal language would seem to make this a requirement.

I might note that in addition to much of this information being relevant for future investigations, often involving the same people, some old investigative and criminal justice files in important cases also have historic value, and some may be retained, I believe, in the Archives.

Some of the most important changes for the better in our criminal justice system have been in part due to the retention of historic investigative and criminal case files. And those apparently would be lost forever under S. 2008.

S. 1428, on the other hand, does not mandate destruction or complete purging, if you will. Rather, it tries to get at the problems involved with who gets access to investigative files.

Of course, both bills emphasize certain concepts in regard to criminal justice cases with the obvious high purpose of achieving protection of individual privacy and the protection of society through legitimate law enforcement.

Both bills are concerned with accuracy. Both bills stress the reporting of dispositions of criminal charges and the right of access of an individual to criminal history information in order to correct inaccuracies in such information. Both bills, albeit somewhat differently, provide an incentive to report dispositions by restricting access to and dissemination of stale arrest records.

But we have already noted that the bills define "disposition" in quite different terms. S. 1428 includes as a "disposition" any action which permanently or indefinitely disposes of charges. This would include, therefore, such things as incompetence to stand trial, pretrial diversion, dismissal in favor of a civil action, and so on. S. 2008, however, defines "disposition" to include a decision not to bring criminal charges, or a conclusion or abandonment of criminal proceedings.

Let us note one significant problem with respect to S. 2008 providing for access to and correction of records. Section 209 of that bill requires a criminal justice agency not only to grant access, but also to correct records it possesses. But that bill in that section does not differentiate, as does S. 1428, between records originating in the agency having possession, and records originating elsewhere.

Thus, there may be a serious problem where, let's say the FBI, or another Federal agency, has a large number of State records in its possession, records which it has neither the authority nor the information to correct. Obviously, therefore, it cannot do any correcting even when it has reason to believe that the individual is entitled to his request for correction.

Accordingly, we think that the better approach is that taken in S. 1428, which squarely places the responsibility of correction on the originating agency rather than on the agency which happens at a given time to have possession of the records in question.

Let me turn now to some matters having to do with the question of accountability. Now, obviously both bills are concerned with accountability. Thus, agencies disseminating information, for example, are required to keep records of who obtained the information, and why. In addition, S. 1428 requires special accounting for remote terminal access to information by street patrols to insure that information retrieved from computers is properly utilized. As the subcommittee knows, with what is going on and the kinds of equipment in patrol cars, this is most important. And we note that there is no such provision or counterpart in S. 2008.

Another aspect of accountability is dealt with by requiring that politically responsible officials make the decisions—and publicly so—as to the propriety of noncriminal justice agencies, particularly employers and the licensing boards, receiving criminal justice information about applicants for employment or licensing.

Dissemination of this information cannot, under the bills, continue on the basis of custom or agency regulation alone.

For example, if trucking companies viewed access to criminal history information as vital to cargo security, they could not determine that unilaterally. They would have to convince a legislature in S. 2008, or a governor under S. 1428, that cargo security is sufficiently important to warrant access to such information.

Moreover, the legislature or governor would be required to decide whether only certain records, such as those showing dispositions would

be available, or whether arrest records, or whatever, might also be made available in these areas. And as I have said, these decisions must be subject to public scrutiny.

The bills do provide access by Federal agencies to criminal justice information for the purpose of providing information for employment or security clearance, although the details of the bills vary considerably.

Incidentally, although I think it is probably already clear to this subcommittee, the reason why the bills focus more particularly on Federal employment is that it was thought, we believe, that this would save additional legislation by the Congress dealing with a responsibility in the Federal sector. Conversely, the bills are not so specific about State or local employment, because this would be a matter for State or local determination subject to the minimum standards provided in these bills.

Nevertheless, the two bills in these areas still differ. For example, S. 2008 would not permit Federal agencies, even Federal law enforcement agencies, to receive investigative information, for example, for employment purposes unless there was a full field investigation for the purposes of access to top secret information. S. 1428, on the other hand, would permit such information to be made available for law enforcement and other Federal employment subject to certain conditions on use. S. 1428 does say, however, that no criminal justice information may be used as a disqualifying factor unless it is reasonably related to the particular employment in question. That bill requires that an employment decision based on criminal justice information be made at a higher supervisory level, not just in a routine fashion.

S. 2008 does not address the use of information by the employing agency.

Now, both bills attempt to take up certain problems of access in certain specific agencies such as, the Immigration Service, various components of the Treasury Department, and so on. S. 1428 provides that criminal history record information—now here we mean, incidentally, information which indicates a disposition of charges and not just an arrest—may be made available to registered drug manufacturers and federally chartered or insured banks. S. 2008 would permit dissemination of "criminal record information," apparently including just arrest records as well as records with the disposition, to drug manufacturers, but contains no provisions with regard to banks.

I might note, Mr. Chairman, that the present law authorizes such institutions to receive both arrest and disposition information. S. 2008 would appear to repeal existing law in this area. But it does not contain a new provision relating to banks.

Now, S. 2008, as noted earlier, establishes a regulatory agency. And we would like to dwell briefly on the problems and considerations here. That regulatory agency would set the guidelines under which all criminal justice agencies in the country would have to operate, whether they be Federal or State. In our view S. 1428, which leaves the task of fashioning rules and procedures to reach the goals set forth in Federal law to each State and local agency, is preferable.

We do think, of course, that the Federal Government should set standards for information which flows interstate. But we do not think that the precise regulations to implement these standards should be set anywhere else than at the State and local level.

Moreover, it is our opinion that it would not be wise or correct for an executive branch regulatory agency to intrude into the management of information systems maintained by the courts at the State or local level, or indeed for that matter, at the Federal level.

Once Congress provides and sets forth the goals, the courts probably should make independent decisions as to how these goals are achieved.

Apart from these legal and separation of powers considerations, I should note once again the practical problems, which would become myriad and almost beyond description, if we were to have a single set of rules imposed by the Federal Government with any specificity. Hence we prefer the approach in S. 1428 of Federal goals and local implementation.

Of course, in fairness I should note that S. 2008 contemplates that State agencies having similar powers to the proposed Federal commission would take over supervision of State and local agencies as to implementation matters.

But these State agencies, nonetheless, would apparently be bound by Federal commission regulations from which they could not deviate. Moreover, we point out that under S. 2008, the commission would expire at the end of 5 years. The State agencies would then be left bound by rigid regulations previously issued and which could not be changed by any machinery that we can see provided for here. Thus the Department would oppose this concept.

Now, I would like to turn as swiftly as possible to the bills' approaches to enforcement, which are quite similar. However, there are some differences in detail, in matters of importance.

Both bills provide injunctive and tort relief for violations of the Act, but make good faith a defense to tort relief applications.

The chief difference in respect to civil remedies is that S. 2008 authorizes the commission itself to seek declaratory judgments or cease and desist orders. This provision, which is not found in S. 1428, would apparently permit the commission to stop a criminal investigation or an intelligence investigation at any time to litigate the issue of whether a particular recipient of information had a "need-to-know," or whether, going back to our earlier discussion, the information was maintained on the basis of "specific and articulable facts."

I would suggest most sincerely that this type of interruption would almost certainly abort a trial or an investigation even if it were later determined that the challenge was groundless.

Mr. Chairman, as one who has spent most of my life in the criminal justice system, that is, most of my professional life, I have to state the obvious, that that system grinds on, it seems, almost endlessly now, and if we were to have further interruptions of this kind, no matter what the motive of those who drafted such a proposal, I think this would be intolerable.

I also must note, on the other side of the coin, that under existing law, infringements of constitutional rights of individuals can be challenged in the courts. Thus, in my judgment and the judgment of the Department of Justice, adequate remedies are available without taking this type of approach. Hence, we strongly oppose this part of S. 2008.

Let me turn to the criminal provision of that bill.

As you know, that provision applies to any willful or knowing violation of the act by a government employee. S. 1428's criminal provision applies only to unauthorized disclosure of intelligence or investigative information, in knowing violation of a duty imposed by law.

Now, here we have carefully considered the bills and have concluded that the broader penalty approach taken by the draftsmen in S. 2008 probably is preferable. In other words, we do not think that there is any really powerful reason for differentiating between unauthorized disclosure of criminal record information, on the one hand, and intelligence and investigative information on the other.

We do not, however, consider that the culpability standard of S. 2008's provisions are adequately defined. Hence, we have taken the liberty of proposing to the subcommittee alternative language for a new criminal provision in S. 1428. This is attached, as you know, to our printed testimony, as appendix A.

Let me turn to another enforcement difference between the two bills which we think is very important. S. 1428 provides that nothing in the act or regulations or procedures adopted to implement it can provide a basis for excluding otherwise admissible evidence in court.

The parallel provision in S. 2008 is limited to violations of internal operating procedures adopted by agencies, thereby suggesting that any violation of the act itself, or of commission regulations, that is, federal commission regulations, would provide a basis for application of the exclusionary rule in the trial of a criminal case.

We do not think that this is a wise or salutory idea at all, nor will it be of any help realistically in protecting individual constitutional rights. Thus, we do not advocate and strongly oppose, as a matter of fact, any extension of this so-called exclusionary rule principle.

Now, Mr. Chairman, I have already mentioned the compendium, of which we will provide additional copies, as suggested by Senator Hruska, for the Committee as a whole. And I will conclude by reiterating that we share the goals which the draftsmen in both bills obviously have in mind. Nevertheless, we remain strongly in support of S. 1428 as opposed to S. 2008, a more recent version here discussed this morning.

I would welcome any questions by you, sir, or by any member of the subcommittee, or by subcommittee counsel.

[The prepared statement of Hon. Harold R. Tyler, Jr., follows:]

PREPARED STATEMENT OF HON. HAROLD R. TYLER, JR., DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to appear before this Subcommittee to discuss S. 2008, the "Criminal Justice Information Control and Protection of Privacy Act."

Legislation relating to the protection of privacy with respect to criminal justice information is a matter of high priority with the Department of Justice and with other Departments and agencies concerned with law enforcement.

The Department of Justice began drafting legislation on the subject of the exchange of criminal justice records in 1971. A new and broader proposal submitted in February 1974, placed greater emphasis on individual privacy than had earlier bills. We were unable to obtain Administration clearance since other agencies were dissatisfied with this proposal. However, in November 1974 we submitted

a total revision of our criminal justice privacy bill to the Congress, this time as an Administration bill. This final proposal, Mr. Chairman, you introduced on April 14 as S. 1428. I review this history to emphasize the complexity of the issues involved in balancing the interests of the administration of criminal justice and rights of personal privacy and our own struggle with these issues. We are satisfied that the proper balance is struck in S. 1428 and we strongly support its enactment. We are unable to support S. 2008, in its present form, both because of technical drafting problems and because of fundamental disagreement with some of the concepts it embodies.

I.

All legislation designed to protect individual rights of privacy involves a tension between the public's right to know and the individual's right to preserve a certain zone of privacy into which the public cannot intrude. Nowhere is this more evident than in legislation dealing with criminal justice information. If records of arrests, court proceedings, and correctional decisions are not publicly available, then the public is not only generally uninformed about its criminal justice process, but individuals risk all of the dangers inherent in secret arrests, star chamber proceedings, and banishment to secret prisons. Yet if a past error, already paid for, can follow an individual for the rest of his life, threatening his employment opportunities and his acceptance in the community, our hopes of rehabilitating offenders through improved correctional services are impeded. Both S. 1428 and S. 2008 attempt to accommodate these concerns by preserving public access to police blotters, court records, sentencing and parole decisions, but denying public access to the centralized and compiled history of such matters, identified by individual name.

Traditionally, law enforcement in the United States has been a matter of State and local concern, with Federal law enforcement jurisdiction carefully circumscribed. At the same time, Federal, State and local law enforcement agencies continue to cooperate with each other on matters of common concern and routinely exchange information of mutual interest. The advent of the computer has increased the capability for this exchange of information and reinforced the interdependence of law enforcement agencies throughout the country. Recognizing this, both bills extend not only to federal agencies but also to State and local agencies which operate with federal funds, exchange information interstate, or exchange information with federal agencies.

S. 1428 also recognizes the primacy of State and local government in the criminal justice area by avoiding the imposition of strict federal controls on the operations of criminal justice agencies. S. 2008, on the other hand, establishes a federal commission to oversee administration and enforcement of the provisions of the bill with power to issue binding federal regulations, interpretations and procedures. While the bill encourages creation of State agencies to perform these functions within a State, those agencies would be bound by the federally-established guidelines. In our view, this approach intrudes too deeply into the primary responsibility of the States for the administration of criminal justice.

Of all the areas of competing values which must be addressed in such legislation, perhaps the most difficult is striking the proper balance between the protection of society and the preservation of individual privacy. In most repects, neither bill attemps to do this. Rather, each requires that the politically responsible officials at the Federal and State levels decide on a case-by-case basis whether it is more important that a potential employer know of a past criminal record or that the prospective employee's privacy be protected. S. 2008, however, circumscribes the extent of this decision-making by foreclosing access to certain records and providing for the sealing or destruction of other records. Moreover, it permits decisions on access to be made only by the legislature at both the federal and State levels. S. 1428, on the other hand, permits a decision to make records available to be made by the chief executive as well as the legislature at both Federal and State levels. This decision could extend to all criminal justice records, not just certain types, so long as the decision is made on the public record and specifies the types of records to be made available.

II.

With this introduction, let me outline some of the fundamental concepts involved in these bills and explain our objections to S. 2008.

The basic difference in approach between S. 1428 and S. 2008 is that the latter attempts a comprehensive regulation of criminal justice information—forbidding

uses not specifically authorized. S. 1428 does not purport to be comprehensive. It establishes certain goals, provides some minimum standards, and focuses on identifiable problems, leaving room for further refinements as experience is gained and the expertise developed. For example, S. 2008 specifically enumerates the only purposes for which arrest records may be exchanged among criminal justice agencies, thus precluding all other exchanges. S. 1428 does not attempt to anticipate or enumerate all of the valid uses of arrest records; rather, it focuses on such problems as the misuse of arrest records in determining probable cause and unrestricted access to computerized records by street patrols. Having focused on these specific problems, it leaves the determination of other valid uses to the individual criminal justice agency.

Quite frankly, despite the number of years we have worked on issues of criminal justice information and privacy, we do not feel that we are in a position to enumerate all uses of criminal justice information. We believe it would be premature to apply the preclusive approach of S. 2008 to the thousands of State and local criminal justice agencies that would be covered by this legislation. In our view, it is far wiser to address the specific problems identified to date and establish a mechanism, such as the Commission proposed in S. 1428, to recommend refinements in the future.

Both bills recognize the interdependent and interconnected role of Federal, State and local criminal justice agencies, but the approach differs. S. 1428 would apply a uniform federal standard to interstate exchanges of information and exchanges between federal and State agencies. At the same time, it recognizes the primacy of State law within the State boundaries so long as the State law meets the minimum federal standards. S. 2008 provides that State law will govern all maintenance, dissemination and use of information within the State insofar as it imposes stricter standards than the Federal law. It suggests that such State laws will regulate not only State and local agencies within the State but also federal agencies located within the State boundaries. It could also be read to impose restrictions on information found within the State even though it originated in an agency of a different State or in a federal agency outside the State. It might even be interpreted to apply to information being exchanged by two States but passing through the State with the stricter State law. There is some question whether States, even with the permission of Congress, can impose standards on the use and dissemination by federal courts of information acquired, maintained or used by those courts simply because of their physical location within the State. Issues of federal supremacy and separation of powers are clearly raised by such a provision. Aside from the constitutional issues, the practical effect of such a provision is chaotic.

Both bills extend to all major aspects of criminal justice information—criminal histories, investigatory and intelligence information, and correctional information—and both address to some degree the collection, retention, use and dissemination of this information. The bills differ substantially, however, in the degree of specificity with which they regulate this information and in the number of subcategories into which they divide it. The differences in definitions make it particularly difficult to compare the two bills. S. 1428 speaks of "arrest record information," which has no disposition attached, and "criminal record information," which means that a disposition is attached. It defines "disposition" with some specificity. It uses the term "criminal justice information" to encompass all types—arrest and criminal record information, correctional information, and investigatory and intelligence information. S. 2008 refers to "arrest record information," "nonconviction information," "conviction record information" and "criminal history record information," with the latter term unclear as to which of the former it encompasses. It uses "criminal justice information" to mean the terms mentioned above plus "correctional and release information" but has no general term to encompass all types of information. Moreover, S. 1428 defines "disposition" to include a variety of procedures for terminating a case, including pretrial diversion, while S. 2008 uses the same term to mean only a dropping of charges or a conviction.

More fundamental than the definitional distinctions is the difference in treatment of intelligence information in the two bills. S. 1428 is cast in general terms, restricting intelligence collection to official purposes, limiting access on a need-to-know basis, and requiring an accounting of exchanges with other agencies. S. 2008 attempts to define standards for maintenance and dissemination of intelligence. Maintenance—a term not defined—would be authorized only if "grounds exist connecting such individual with known or suspected criminal activity and if the information is pertinent to such criminal activity." Information could be dis-

seminated to another agency only to confirm information in the other agency's possession or for investigative purposes if the other agency can "point to specific and articulable facts which taken together with rational inferences from those facts warrant the conclusion that the individual has committed or is about to commit a criminal act." We have real difficulties with these "standards" because of their vagueness and the difficulty of applying them in the intelligence context. The articulable fact standard is borrowed from *Terry* v. *Ohio*, 392 U.S. 1 (1968), the stop and frisk decision. While the standard provides guidance for the policeman on the street in deciding whether to pat down a suspect, we seriously question whether the same standard has validity when determining what information can be volunteered to the Secret Service concerning a potential assassin.

As S. 2008 is written, dissemination to another agency is authorized only to confirm information that agency already has or when the articulable fact standard is met. But the nature of intelligence is such that bits and pieces of information of a seemingly unconnected nature must be pieced together until the whole picture is formed. If dissemination cannot be made in an organized crime case until there is confirmation that the requesting agency already has the information or has facts relating to a criminal case which relate to specific criminal activity, then our present efforts against organized crime must be shut down completely.

The standard for "maintaining" information creates equally great problems. When received by a law enforcement agency, a first item of information may not yet have any established connection with criminal activity, though verification of the information might reveal such a connection. Further inquiry is required to determine whether the item is true and whether it warrants further investigation. If that information cannot be "maintained" long enough to verify it, then no investigation may ever be begun. If it may be maintained for a brief period but never recorded in files, then there will never be a record of the investigations conducted and review and oversight will be effectively avoided.

In our view, the proposed "standards" in S. 2008 for both maintenance and dissemination of intelligence are unreasonable and unworkable.

We do not suggest that standards for intelligence collection and dissemination should not be established. As you know, the Department of Justice is now attempting to formulate guidelines for the FBI with respect to intelligence collection, retention, use and dissemination. But the further the Department's committee probes the issues, the more complex they appear. It will be some time before we can formulate adequate guidelines for the FBI, with its limited jurisdiction. It is even more difficult to set standards for the diverse federal, State and local agencies that would be regulated by these bills. To attempt to formulate such standards in these bills is, in our view, premature. The wiser course is to require agencies to formulate their own guidelines in the first instance, subject to study and recommendation by the proposed commission, as it develops expertise in this most difficult area. This is the approach taken in S. 1428.

The approach to investigative information in S. 2008 poses equally difficult problems. The bill would require that such information could not be maintained beyond the expiration of the statute of limitations for the particular offense or the sealing or purging of criminal history information relating to that offense. Thus, if a marginal securities fraud case is not referred for prosecution, both the criminal history record and any investigative files would be required to be sealed or destroyed and any subsequent investigation of a similar case would have to begin from scratch.

Moreover, an investigatory file would have to be sealed or destroyed upon the running of the statute of limitations regardless of its relevance to later cases. We cannot believe that this is the intent of the bill and yet this is what it requires. I might also note that the bill pays no attention to the possible retention of investigative files for historic or archival purposes. Had it been in effect some years ago, the background on some of the most important criminal cases in our history would be forever lost. S. 1428, in contrast, focuses on the question of access to investigatory files; it does not mandate their destruction.

Both bills emphasize certain concepts with respect to criminal record information designed to achieve the twin goals of protection of privacy and protection of society through effective law enforcement. These include the requirement of accuracy with respect to the information. Both bills stress the reporting of dispositions of criminal charges and the right of access of an individual to criminal history information in order to correct inaccuracies in it. In addition, the bills, in somewhat different fashion, provide an incentive to report dispositions by restricting access to and dissemination of stale arrest records. As noted earlier, however, the bills define "disposition" in very different terms. S. 1428 includes as a "dis-

position" any action which permanently or indefinitely disposes of the charges. This would include incompetence to stand trial, acquittal by reason of insanity, pretrial diversion programs, dismissal in favor of a civil action, etc. S. 2008 defines "disposition" to include a decision not to bring criminal charges or a conclusion or abandonment of the proceedings.

There is one significant problem with respect to the provision for access to and correction of records in S. 2008. Section 209 requires a criminal justice agency maintaining a record not only to grant access but also to undertake the correction of the records it possesses. It does not differentiate, as does S. 1428, between records originating in the agency having possession and records originating elsewhere. This presents serious problems for the FBI which has a large number of State records in its possession—records which it has neither the authority nor the information to correct. We suggest that the better approach is that taken in S. 1428 which places the obligation to correct on the originating agency, rather than on any agency having possession of the record.

A concept common to both bills is that of accountability. Agencies disseminating information are required to keep records of who obtained the information and why. In addition, S. 1428 requires special accounting for remote terminal access to information by street patrols in order to insure that information retrieved from computers is properly utilized. There is no comparable provision in S. 2008.

Accountability is also provided by requiring that politically responsible officials make public decisions as to the propriety of noncriminal justice agencies, particularly employers and licensing boards, receiving criminal justice information about applicants. Dissemination of this information could not continue on the basis of custom or agency regulation. For example, if trucking companies or warehousemen viewed access to criminal history information as vital to cargo security, they would have to convince a legislature, or in the case of S. 1428 a Governor, that cargo security is a sufficiently important interest to warrant access to such information. Moreover, the legislature or Governor would be required to decide whether only certain records, such as those bearing dispositions, should be available or whether access to arrest records is also warranted. These decisions would, of course, be subject to public scrutiny.

The bills specifically provide for access by federal agencies to criminal justice information for the purpose of providing information for employment or security clearance although the details of the bills vary considerably. For example, S. 2008 would not permit federal agencies, even federal law enforcement agencies, to receive investigative or intelligence information for employment purposes unless there was a full field investigation for purposes of access to "Top Secret" information.

S. 1428 would permit such information to be made available for law enforcement and other federal employment subject to certain conditions on use. S. 1428 specifies that no criminal justice information may be used as a disqualifying factor for employment unless it is reasonably related to the particular employment and requires that an employment decision based on criminal justice information be made at a higher supervisory level, not in a routine fashion. S. 2008 does not address the use of information by the employing agency.

Both S. 1428 and S. 2008 specifically address certain other access by federal agencies, such as the Immigration Service and various components of Treasury. S. 1428 provides that criminal record information, that is information which indicates a disposition of charges and does not merely reflect an arrest, may be made available to registered drug manufacturers and federally-chartered or insured banking institutions. S. 2008 would permit dissemination of "criminal record information"—apparently including arrest records without any disposition—to drug manufacturers, but contains no provision with respect to the financial institutions. I might note, Mr. Chairman, that present law authorizes such institutions to receive both arrest and disposition information. While S. 2008 would repeal the present law on this subject, it does not contain a new provision relating to the financial institutions.

Having set minimum standards for criminal justice information and addressed certain specific problems, S. 1428 leaves the task of fashioning rules and procedures to reach the legislatively-defined goals to each criminal justice agency. As noted earlier, S. 2008 establishes a regulatory agency which would set the guidelines under which federal, State and local agencies must operate. In our view, the approach taken by S. 1428 is preferable as a matter of principle and necessary as a practical matter. Our system of government rejects the idea of federal intrusion into the management and operation of State and local agencies. It is appropriate for the federal government to set standards for information which flows interstate

but the precise regulations to implement those standards should be set at the State and local level. Moreover, it would be inappropriate for an Executive Branch regulatory agency to intrude into the management of information systems maintained by the courts at either the federal or State level. Once the goals of Congress are articulated, the courts must be allowed to make independent decisions as to how those goals are achieved. Aside from these fundamental principles of federalism and separation of powers, the very diversity and complexity of the many federal, State and local criminal justice information systems covered by the bill necessitates that each be allowed to fashion regulations tailored to its particular systems. Considering that the bills apply to records of law enforcement, prosecution, corrections and courts, and that they encompass manual, semi-automated, and fully-automated systems, it becomes apparent that a single set of rules imposed by the federal government cannot possibly apply with any specificity. It is for these reasons that S. 1428 adopts the federal goal—local implementation approach.

It is true that S. 2008 contemplates that State agencies having similar powers to the proposed federal commission would take over supervision of State and local agencies as to implementation of the bill, but these State agencies would be bound by Commission regulations and interpretations from which they could not deviate. Moreover, once the proposed Commission expires at the end of 5 years, these State agencies would be bound by rigid and unchangeable regulations, previously issued, regardless of changes in circumstances. The Department cannot support this concept.

I have just outlined some of the fundamental differences between S. 2008 and S. 1428. The former leans toward a comprehensive code approach. S. 1428, on the other hand, does not attempt to reach all areas of information practice to which federal power might extend, or to resolve all issues. Rather, it is a beginning and one which presupposes future change and refinement as new problems are identified, new technologies developed, and knowledge of the diverse information systems and their uses increases. The Department of Justice is convinced that this is the wiser course at this time.

III.

The two bills have a similar approach to enforcement, except for differences in the proposed commission. They visualize civil remedies and criminal penalties. The details differ considerably, however, and in matters of some importance.

The bills provide injunctive and tort relief for violations of the Act but make good faith a defense to tort relief. The chief difference with respect to civil remedies is that S. 2008 authorizes the commission itself to seek declaratory judgments and cease and desist orders. This provision, not found in S. 1428, would permit the commission to stop a criminal investigation or an intelligence investigation at any time to litigate the issue of whether a particular recipient of information had a "need to know" that information or whether the information was maintained on the basis of "specific and articulable facts." Such an interruption would almost certainly abort the investigation itself, even if the challenge were found to be groundless. In the view of the Department, the criminal justice systems in this country cannot tolerate such potential interruptions of investigations at this early stage. Infringements of constitutional rights during investigations can be, and are, challenged at the prosecutive stage and this has proved adequate to protect individual rights. The Department is strongly opposed to this provision of S. 2008.

The criminal provision of S. 2008 applies to any willful or knowing violation of the Act by a government employee. As written, the criminal provision of S. 1428 applies only to unauthorized disclosure of intelligence or investigative information, in knowing violation of a duty imposed by law. We have concluded that the broader penalty approach is preferable. There is not a valid reason for differentiating between unauthorized disclosure of criminal record information and correctional and release information, on the one hand, and intelligence and investigative information on the other. We do not consider the culpability standard of S. 2008 adequately defined, however, and we have developed alternate language for a new criminal provision in S. 1428 which is attached as Appendix A of this testimony.

There is another difference in the enforcement provisions which we consider critical. S. 1428 provides that nothing in the Act or regulations or procedures adopted to implement it can provide a basis for excluding otherwise admissible evidence in court. The parallel provision in S. 2008 is limited to violations of internal operating procedures adopted by agencies, thus suggesting that any violation of the Act itself or of commission regulations would provide a basis for the exclusion of valid evidence in criminal proceedings. In a bill as far reaching and sweeping as this, such an extension of the exclusionary rule is intolerable.

IV.

The Department of Justice strongly supports S. 1428 and urges Congress to give it prompt attention. For the reasons suggested in my testimony, as well as a number of technical drafting problems which we have not enumerated, we cannot support S. 2008.

When criminal justice privacy legislation is enacted, we urge that it be the sole basis for regulation of such information and that criminal justice information be excluded entirely from the coverage of the Privacy Act of 1974. This is obviously your intention, Mr. Chairman, since section 314 of S. 2008 seeks to accomplish this. We should point out, however, that, as written, section 314 has the effect of repealing the Privacy Act entirely—a result not intended. We have alternate language to suggest, in Appendix B, which would accomplish the intended effect.

Finally, Mr. Chairman, the Law Enforcement Assistance Administration has prepared a Compendium of State laws on criminal justice and privacy. The Committee may find it useful in connection with your efforts on this legislation and I will be happy to provide you with a copy today.

Again, I appreciate the opportunity to discuss this important legislation with you and to express the Department's deep concerns about S. 2008. I will be happy to respond to any questions you may have.

APPENDIX A

Proposed new criminal provision in S. 1428.

Delete subsection (f) of § 209, add a new section 309, and renumber existing sections 309 through 312 as 310 through 313.

"Sec. 309. A person is guilty of a misdemeanor if he knowingly discloses criminal justice information to which he has or had access in an official capacity, to a person not authorized by law to receive such information, in violation of a specific duty imposed upon him as an officer or employee or former officer or employee of government, by statute, or rule, regulation or order issued pursuant thereto. The offense shall be punishable by imprisonment not to exceed one year, a fine of not to exceed $10,000, or both."

APPENDIX B

Proposed new section 314 removing criminal justice information from the scope of the Privacy Act of 1974.

"Sec. 314. (a) The provisions of section 552a of Title 5, United States Code are amended:

(1) By deleting the word 'criminal' in paragraph (4) of subsection (a);

(2) By amending subsection (j) by striking the dash in the first sentence thereof, deleting the designation (1) and deleting the '; or' and inserting in lieu thereof a period, and by deleting all of the paragraph numbered (2); and

(3) By striking from paragraph (2) of subsection (k) the words 'subsection (j)(2) of this section' and inserting in lieu thereof, 'the Criminal Justice Information Control and Protection of Privacy Act of 1975.'

(b) Section 5 of the Privacy Act of 1974, Public Law 93-579, is amended by striking the period at the end of clause (C) or paragraph (2) of subsection (c) and adding at the end thereof, 'or subject to the jurisdiction of the Commission on Criminal Justice Information."

Senator TUNNEY. Thank you, Mr. Tyler.

We have about 20 minutes, Senator Hruska. I suggest that we go on a 10-minute rule. I will ask questions for 10 minutes, and then turn it over to you. If we have more time, we will just keep going on that basis.

Senator HRUSKA. That is gracious of you.

Senator TUNNEY. I appreciate very much, Mr. Tyler, your testimony. I notice that you have given considerable thought to the language in the two bills, and on the committee we are going to give great attention to the specific suggestions you have made.

However, as I read your testimony last night and then heard it again this morning, I perceive that there is a basic disagreement over the thrust of the Justice Department position and my position. In

my opinion, and somewhat in contrast to your testimony, the latest subcommittee bill, S. 2008, returns much more power to the State and local levels of government than does the latest Justice Department bill, S. 1428. Now, there are certain areas where there is a difference, where we would not return that power to the States in the same way that you do. But the basic thrust of all this legislation is that it would turn more power over to the States.

Would you comment?

Mr. TYLER. I think, as we read it, the draftsmen may well have intended that. However, we are not too sure that the bill really comes out that way. In other words, I do not have any quarrel with the apparent intentions of S. 2008. And yet as we read the drafting, we are not sure by any means that the State and local agencies are going to be allowed to do the implementation without a considerable amount of direction by the Federal commission as proposed in S. 2008. Now, as I said, however, I accept your statement, Mr. Chairman, that that was really not the intention.

Senator TUNNEY. Since your testimony shows disagreement as to the language that we have used in S. 2008, I feel that the staff of this subcommittee, and staffs of interested Senators, and representatives of the Justice Department should meet and go over both bills on a section-by-section basis, to get a better understanding of what we intend to accomplish with S. 2008. We cannot do it here.

Mr. TYLER. I think that is correct.

Senator TUNNEY. We have to discuss in the broadest sense the basic issues. I think that would be important.

I notice that you have persons working for you in the Department who are totally familiar with both bills and who would be able to sit down with the staff on this subcommittee and the staffs of individual Senators, even the Senators themselves, to work out the specific language. If we cannot agree we cannot agree, and we can just take the votes. But at least we would know precisely where it is we disagree and where, in your view, we may not have been effective in writing adequate standards.

Mr. TYLER. As you know, Mr. Chairman, this would be perfectly fine, particularly since it is so hard to draft tight definitions.

This is not easy. You know that, and we know that as well. And so that kind of meeting later would be just fine, if that is what the subcommittee and the staff would wish. We would be in a position to welcome anything like that.

Senator TUNNEY. I feel that it is important.

I have heard from unimpeachable sources that the FBI was experimenting a little over a year ago with using NCIC for intelligence purposes, the idea being to use the enormous traffic in the NCIC, whether generated by the FBI, or the users of the systems, to keep track of individuals that might be of interest to the FBI for whatever purposes, including possibly political reasons.

My understanding is that the FBI cut off the experiment 2 days before Senator Ervin began hearings last March on this same legislation. Apparently the impact of the Watergate scandals served to stop this potential abuse. I have developed 10 questions which I had hoped would enable us to cover this episode. Obviously we do not have time to get all your responses, and you should have time to evaluate them

to make sure that you are familiar with the facts, and I would like to have you report all the facts back to us.[1] I will read them now.

1. Is the practice of using flags a common practice among criminal justice identification units?

2. Has the FBI used flags in its manual identification operation?

3. If so, what criteria are used to flag an identification card and for whom will the FBI establish a flag in its manual file?

4. Are flags used in the manual system for purposes other than to help locate persons for whom warrants are outstanding? If so, for what purposes?

5. Has the FBI used flags in its NCIC system?

6. What criteria were used to determine which records or individuals were to be flagged in the NCIC system?

7. To what extent could other Federal, State, or local agencies request that flags be placed on the information in the NCIC system?

8. To what extent could divisions within the FBI request that flags be placed?

9. Were flags ever used in the NCIC system for purposes other than to help locate persons with warrants outstanding, such as for allowing the FBI or other criminal justice agencies to know the location of certain persons the agencies had an interest in? If so, please explain what such programs were and their duration.

10. Given the FBI's experience in using flags, what issues are under active consideration by NCIC about their use?

I am going to submit these questions to you and let you respond. Would you care to give us any preliminary indication of what you know about this?

Mr. TYLER. I am frank to say that I cannot answer any of those sample questions. However, as you suggest, if you would have someone turn them over to me or one of my assistants, we will endeavor to get the answers.

I had not any more than heard by at least triple hearsay this allegation that you repeated here this morning, and apparently for that reason, and partly because I did not anticipate we would get into the actual NCIC-FBI practices this morning, I am totally without knowledge or information with which I could even give a partial answer. But I am sure we can look into it and try to treat specifically whatever the 10 questions call for.

Senator TUNNEY. Fine.

I have additional questions with regard to the FBI's planned message switching which I will also make available to you for your consideration and for your response.

I think these questions and the subject matter are pertinent to the legislation before us. I strongly feel that we should have a commission which is weighted with State and local law enforcement authorities in their policymaking for the purposes of managing any computer system which will be operated by the FBI or some other agency at the Federal Government level. The possibility of abuses of such a system are such that we ought to have this kind of control. That is the reason the questions are being put to you. I would like, after you have had an opportunity to respond to those questions, to discuss this with you further, and certainly, as we are working on specific sections of the bill, with the Department of Justice and with you personally.

[1] See appendix, p. 288.

Senator Hruska.

Senator HRUSKA. May I suggest that you proceed, Mr. Chairman, because you have authorship of these bills, and I know you have other questions you would like to put to Mr. Tyler.

Senator TUNNEY. Thank you, Senator. I would be more than happy. We have probably 10 minutes.

Senator HRUSKA. You go ahead.

Senator TUNNEY. Very well.

I was interested in the statement that you made that we expand the exclusionary rule in our bill. And yet section 308(g) on page 35 of S. 2008—I am now reading subsection (g):

> A determination by a court of a violation of internal operating procedures adopted pursuant to this Act should not be a basis for excluding evidence in a criminal case unless the violation is of constitutional dimension or is otherwise so serious as to call for the exercise of the supervisory authority of the court.

I thought that by including that subsection we were taking care of the problem that you addressed in your statement. Would you care to comment?

Mr. TYLER. Well, we read that very simply to be nothing other than a statement of the exclusionary rule principle itself. In other words, the exclusionary rule as I understand it as a lawyer would only be brought into play if there was a violation of constitutional dimensions, or as it is put here, otherwise so serious as to call for the exercise of the supervisory power of the court. In other words, the limiting language earlier really is legally meaningless in my opinion. Therefore, it is not realistically a successful attempt to limit the exclusionary rule principle at all. And that is what concerns us.

Perhaps I have not put that succinctly enough, Mr. Chairman.

Senator TUNNEY. If you will state it again, I think I understand——

Mr. TYLER. Subsection (g) says that the exclusionary rule should not be applied "unless the violation is of constitutional dimension or is otherwise so serious as to call for the exercise of supervisory powers."

My understanding as a lawyer is that that is the only time that you would have the exclusionary principle come up in any event. And therefore, it is not really a limiting provision as the draftsman may have intended it to be. That is our view of the matter.

Senator HRUSKA. Mr. Tyler, in reference to section 308(f), which pertains to suits against the United States, do we have any comparable provision in any other law where there is blanket consent by the United States to be sued for violation of the law under which the proceedings go forward? I know of none offhand. I wonder if there is precedent for that, and if it will become, perhaps, a very bad precedent.

After all, the laws of the United States overule those of any State. The ability to defend itself from unwarranted suits and unforeseen results is held in pretty high order of priority. Here is an effort made, in the form of a blank check, to permit the United States to be sued at any time on account of the provisions of this act.

Mr. TYLER. Yes. And there is another aspect of subsection (f) which is related to your point. Normally, particularly in modern times, where you are attempting to provide penalties where an individual such as a police investigator or some agency will fully violate a statute of this kind, it does not always mean that the United States itself should be responsible. So that you have got that aspect to your question, too, which is troublesome.

First, I don't know of any situation or any act which has quite this provision where the United States is deemed to consent to suit. Furthermore, I think it is particularly peculiar in this type of an area where the thrust of the bill as a whole is to get at the individual officer or agent of a government, such as an FBI agent, a DEA agent, or whatever, in the Federal panoply, and hold him individually responsible to some standard. It seems a little odd to me that under those circumstances, with that particular thrust of this type of a bill, that the United States would be deemed to consent to the suit.

Senator HRUSKA. Thank you, Mr. Chairman.

Senator TUNNEY. Thank you.

Mr. Tyler, I have many questions that I would like to ask you. Unfortunately, however, because of the press of the Senate business today, and because we have another witness, I'm going to have to ask you to excuse me from asking you those questions orally, but we will submit them to you in writing. And hopefully when you respond in writing at that point we will be able to get together.

Mr. TYLER. We will be glad both to respond to them in writing and also to get the people together.

Senator TUNNEY. Fine. Thank you very much.

I know that you want a bill, and we want a bill. I don't think that you are prepared to make concessions that you consider fundamental. In those areas that I consider fundamental I certainly want to have a vote of this committee. And if you cannot agree, you will just have to see what the wisdom of the committee and the wisdom of Congress is.

Of course, the executive branch reserves the right to veto the bills.

Mr. TYLER. May I say—and I know you are aware of this because of our private discussions in this general area—first of all, though the approaches are different, I sincerely believe that in the last 4 years the efforts of this subcommittee and the Department and others have brought all of us closer together, and we may not be as far apart as it may appear.

Second, I would most earnestly make the point, which again I know that you and Senator Hruska and others are aware of, that it would be so helpful to all the State and local law enforcement agencies if we could come up with a resolution here. They have been waiting, and there are some signs that they are growing impatient with us, because we have been waiting for 4 years or more.

I know you are aware of that. And I know how important you know their concern is.

Thank you very much for allowing us to appear today.

Senator TUNNEY. Thank you, Judge.

Our next witness is Mr. Aryeh Neier, executive director, American Civil Liberties Union.

Mr. Neier, we have until 10:30 before we have to adjourn. Would you please proceed?

## TESTIMONY OF ARYEH NEIER, EXECUTIVE DIRECTOR, AMERICAN CIVIL LIBERTIES UNION

Mr. NEIER. I am aware of the stricture of time. I will submit a statement for the record and then summarize and elaborate very briefly on one or two points in my testimony.

First, unlike the last witness, I don't think comprehensive legislation in this area is premature. It is long overdue. The FBI has been disseminating arrest records and conviction records for nearly 51 years. And, millions of people are stigmatized by arrest records and conviction records. S. 2008 is a very valuable piece of legislation in trying to remove the stigmas which prevent so many people from integrating themselves into our society, and from getting jobs and other benefits.

S. 2008 addresses the problem of fairness. It seeks fairness for the individual in not allowing an arrest not followed by a conviction to permanently cripple that person. It also seeks fairness for society in the sense that society cannot afford to have so many people unable to get jobs. They are almost required to live on the margins of society, and to engage in criminal behavior because they are unable to obtain employment, licenses or other things one needs to live in our society.

My criticism of S. 2008, to the extent that I have criticism, is that it doesn't go far enough. It leaves loopholes which I think ought to be eliminated from the legislation.

Let me touch very briefly on some of those loopholes.

S. 2008, in deference to a claimed right of press access to arrest and conviction records, makes police blotters available for inspection. I think this is a mistake. I don't think there is any right of access to police blotters by the press. If it finds out about arrests the press, of course, is free to publish what it will. There should be no possible penalty on the press. But I don't think the Government should be in the business of making available arrest records to the press. I'm sure you are aware that many newspapers routinely publish information on all arrests which took place within the previous 24 hours within that community. It will become a principal operating method for many employers, credit agencies and the like to use those logs that appear in newspapers as the means of gathering arrest records. They will put them into circulation again and prevent people from getting employment and other kinds of benefits.

Senator TUNNEY. What is the system in Great Britain? I know that in general terms there is a great deal of circumvention of the press during that period leading up to a trial after the arrest. Do you know what the law is?

Mr. NEIER. The press can publish the facts of an arrest when it takes place. There isn't any general access to arrest records, but the press is aware that arrests take place, and then publishes certain factual information about the arrest.

In advance of trial the press is very substantially restricted in what it can publish.

I would not advocate the British system. I think the first amendment gives the press the absolute right to publish what it will. The restrictions I advocate are entirely restrictions on government. I don't think it is the business of the government to give out private information on individuals to the press. The press can find those out if it chooses, but government should not be giving that information out.

For instance, if the press finds out the details of a tax return, the press is free to publish that information. But, the Government shouldn't be giving tax returns to the press.

I would apply the same principles that govern tax returns and other private data to arrest records.

Of course, the press can report course proceedings. The press would be able to disseminate information about the operation of the criminal justice system in that way. But giving the press systematic access to arrest records just leaves one more method for putting those records into circulation. Thereby it defeats the ultimate purpose of this legislation.

Another loophole in this legislation has to do with the National Crime Information Center. I would like for a moment to describe the way I see the National Crime Information Center, and what it has done to American law enforcement.

At this moment the National Crime Information Center has over 186,000 transactions a day, or more than 70 million a year.

The standard operating procedure for a police officer in a car is to stop somebody for a traffic violation, take the license, go back to his own car, write out whatever traffic ticket he has to write and, at the same time, radio the license number of the cars and the driver's name to a terminal hooked up with NCIC. That way, the officer finds out any information NCIC may have on the driver or car. NCIC leads police officers to try to maximize the number of contacts they have with individuals. If the police officer wants more information than is obtained just by radioing the license number and name to a terminal, he is under pressure to make an arrest. The arrest legitimizes a much greater search of the person and the car under the Supreme Court's Robinson Decision in 1973. It also allows a more sophisticated identity check.

One consequence of this is that in 1971, the first year NCIC was fully in operation, there were about 640,000 arrests nationally for drunk driving. Two years later, in 1973, there were 940,000 arrests for drunk driving. There was a 47-percent increase in arrests for drunk driving, not because there had been any greater amount of drunk driving than in 1971, but because of the pressure on police to find excuses for making arrests. In that way they legitimized full searches of the persons arrested and the cars, and full identity checks of the sort that wouldn't be possible in a very simple stop for a traffic violation.

Similarly, marihuana arrests went from 225,000 in 1971 to 420,000 in 1973. We see police essentially engaged in a system of random checks. They try to engage in as many of these as possible to get hits on the NCIC system.

Of those 186,000 transactions a day the NCIC claims that it has about three-quarters of 1 percent hits, which suggests there is no more than random luck involved. They are simply trying to get as many transactions as possible in hopes of getting a hit. If somebody correlates statistically in the mind of a police officer with the likelihood of getting a hit, that is, if a person is black, young, or has long hair, there is more pressure on the police officer to check him out. The police officer stops the car or stops the person on the street for a stop-and-frisk, using a walkie-talkie to radio in the information on the person, and has it checked in seconds with NCIC. If anything turns up, he makes an arrest, and gets further information.

It is very easy to make drunk driving and marihuana possession arrests. All the police officer has to do is say the car was weaving and he has the basis for making a drunk-driving arrest.

The standard procedure in marihuana arrests in cars is for the police officer to say he smelled marihuana smoke. That is the most evanescent kind of evidence. Probable cause is established. The arrest is legitimate. Nobody can say afterward that he didn't smell the smoke. There isn't any lingering proof that the smoke wasn't there.

Now, the problem I see with this legislation is that in sections 201 (b)(1), (d), (f), and (g), it legitimizes the availability of arrest records in all these circumstances. It says that once a person has been detained, that is a legitimate basis for transferring the arrest record, even if the arrest record was not followed by a conviction.

All those people stopped for traffic violations by police for NCIC checks have been detained. Therefore, this legislation allows the availability of arrest records to police officers in those circumstances. I think that enormously promiscuous dissemination of arrest records would defeat the purposes of this legislation.

Another loophole I want to point out is in section 204(b). It allows the use of arrest records not followed by convictions for Federal employment purposes, it does so not only when there is specific statutory authorization but when there is an Executive order. I think the Federal Government has a responsibility to set an example to the States and private employers of adherence to the presumption of innocence.

When there is punishment of the sort involved in denial of employment opportunities because of the existence of an arrest record, it defeats the presumption of innocence. This provision puts the Federal Government in the position of setting a very bad example, instead of setting the example I hope it would set.

I applaud the thrust of this legislation. But I hope you will amend it to eliminate those provisions in it which defeat its basic intent.

Senator TUNNEY. I would like to ask you, Mr. Neier, to comment, if you would—you were in the room when the Deputy Attorney General was testifying—on his basic thrust that somehow the legislation I introduced, S. 2008, involves a greater degree of centralization of authority, and takes away from State and local agencies the power and authority which exists at the present time. He says that his evaluation is that the legislation as drafted, irrespective of the intent of the authors or the draftsmen, really accomplishes that result.

You have had an opportunity to study the legislation. And you have had also an opportunity to study the Justice Department bill, S. 1428. In the basic philosophy or thrust of the two bills—excluding for the moment specific errors of draftsmanship—do you think that Mr. Tyler is correct?

Mr. NEIER. No, I don't think he is correct. First, there is a trend within State legislatures to do something about arrest records. There is legislation in Maine, Massachusetts, Florida, and Connecticut on this problem. Last week the New York State Legislature passed sweeping legislation to try to control the dissemination of arrest records. Illinois and Hawaii also have legislation in this area. All the State legislatures now trying to control the dissemination of arrest records are going to find their efforts unavailing.

The basic disseminator of information is the Federal Bureau of Investigation, and their efforts cannot reach the FBI. Therefore, unless the Federal Government provides restrictions of the sort

contained in S. 2008, the efforts of the State legislatures to curb dissemination of arrest records are going to be defeated.

Senator TUNNEY. What is your impression of section 308 in our bill, which provides for civil remedies against a person who disseminates unauthorized information contained in records, as well as the law which provides for criminal penalties in section 309? Would you care to address these two provisions?

Mr. NEIER. Let me first address subsections (f) and (g) of section 308, because Mr. Tyler commented on those.

Senator Hruska asked Mr. Tyler whether he could think of any other legislation where the United States shall be deemed to have consented to be sued in this fashion. Mr. Tyler couldn't think of any. Among the most recent legislation enacted by Congress was the Federal Election Campaign Act. My recollection of that act, as passed by you in 1974, is that it has a similar provision consenting to suit. In fact the people who file suit are automatically allowed to go to an en banc hearing of a U.S. court of appeals. That provision, consenting to suit, seems to me far more sweeping than what is provided in this legislation. Perhaps that was a lapse of memory on the part of Mr. Tyler rather than any real comment on anything unusual in this legislation.

Second, as to subsection (g), I think its effect is to say that whatever exclusionary rule would be applicable in the absence of this statute is maintained. It does not extend the sweep of the exclusionary rule.

I think Mr. Tyler was right in saying this is the law. But what you are saying is that we are not extending the law. We are simply leaving the law of exclusion the way it is right now.

In general, I think the civil remedies and the criminal penalties that you provide in this legislation are proper. They allow people to try to protect their own rights, and contain the right standards for enforcing criminal penalties when there is a knowing violation of the law.

Senator THURMOND. Mr. Chairman, I have another committee meeting. I would like to make an additional comment.

The Deputy Attorney General testified this morning. Did he go into his written statement thoroughly?

Senator TUNNEY. He read almost all of it. There were some phrases and sentences that he did not read, but for the most part, he did go over it all.

Senator THURMOND. He has contrasted S. 1428 with S. 2008, I believe. And he made some very pertinent comments here which require most careful consideration of our committee. For instance, he says:

> S. 1428 also recognizes the primacy of state and local government in the criminal justice area by avoiding the imposition of strict federal controls on the operations of criminal justice agencies. S. 2008, on the other hand, establishes a federal commission to oversee administration and enforcement of the provisions of the bill with power to issue binding federal regulations, interpretations and procedures. While the bill encourages creation of state agencies to perform these functions within a state, those agencies would be bound by the federally-established guidelines. In our view, this approach intrudes too deeply into the primary responsibility of the states for the administration of criminal justice.

Now, I am a thorough believer in the division of powers between the Federal Government and the States. Whatever we do in the criminal justice field should be restricted to the power of the Federal

Government. I don't think we ought to pass any law that is going to intrude on or constitute an invasion of the rights of the States to handle these matters. If we do, we establish a new precedent, something that has never been done before in the 200 years of our country. If we attempt to do this, we will deprive the States of the authority given them under the Constitution.

Regardless of who testifies, I think this subcommittee and the full committee have got to take a hard look at this matter. We certainly want to protect the privacy of persons where it should be protected.

On the other hand, how are we going to protect society, which I put ahead of the individual if we have to choose, because society as a whole deserves the greatest possible protection. How are our homes going to be protected, and how are the people on the street going to be protected, and how is the public in general protected, if we put the right of an individual above them? Now, I realize that we all want to protect the right of the individual, as I most certainly do, but we must not put that goal above the public interest and above that of society as a whole.

I realize that some organizations do not agree with me on this point. I am not too sure that the gentleman present this morning who represents the ACLU agrees with me in this regard. I don't know whether he does or not.

Mr. NEIER. May I comment, Senator?

Senator THURMOND. Yes, you may.

Mr. NEIER. I think the Federal Government is now overriding the States. It is doing so because 10 or 12 State legislatures have recently passed bills trying to restrict the availability of arrest records. Yet, the Federal Government, as the principal source of these records, continues to disseminate them to public and private agencies within those States. It does so despite the wishes of the particular State legislatures. Inevitably, because the Federal Government has the central mechanism for disseminating these records, it is going to set the standard for the Nation as a whole. The question is not whether the Federal Government overrides the State legislatures. The only way it would not override the State legislatures would be if the Federal Government stopped disseminating these records. The question is, which way is the Federal Government going to act? Right now it is overriding some State legislatures which have opted for privacy. Under this legislation it would override some State legislatures which have not yet confronted the question of privacy. But one way or another the Federal Government is calling the tune.

As for the protection of society versus the individual, I do not think that is the choice before us. This legislation is designed as much to protect society as the individual. We just cannot afford to have the enormous recidivist population of millions of people who are not in the labor market because their arrest records prevent them from becoming employable citizens. We cannot afford to have so many social lepers, so many pariahs in our midst, as at present.

While we become more efficient in disseminating these records, and supposedly protect ourselves against crime, we also see a soaring crime rate. And I think the two are directly connected. I don't think the dissemination of records helps prevent crime, I think it helps create crime by making people unemployable.

[The prepared statement of Mr. Aryeh Neier, follows:]

PREPARED STATEMENT OF ARYEH NEIER, EXECUTIVE DIRECTOR, AMERICAN CIVIL LIBERTIES UNION

My name is Aryeh Neier. I am Executive Director of the American Civil Liberties Union and I appear here today on behalf of the A.C.L.U. The American Civil Liberties Union is a nationwide organization of more than 275,000 members devoted to the protection of the Bill of Rights.

I have long been interested in the subject of S. 2008 and I have testified, spoken and written about criminal justice information on numerous occasions. My book, *Dossier*, published in January, 1975, is largely devoted to recounting the injuries done people by the promiscuous dissemination of criminal justice information.

The adoption of S. 2008 would be a major step forward in protecting individual rights. As such, the American Civil Liberties Union endorses this bill. At the same time, we propose several changes. They would enhance the value of this legislation in limiting the use of criminal justice information to unfairly deny people jobs, licenses and intrude on their privacy. Before discussing the specific features of S. 2008, we offer some general comments on the values and social policy considerations at stake.

Arrest and conviction records are collected and disseminated in the belief that such practices are necessary to control and reduce crime. At the same time, there is a growing recognition that the right to privacy and the right to employment are severely damaged by dissemination of such records. If both of these propositions were accurate then the task before you would be to weigh the competing interests and draw legislation accordingly.

On the basis of extensive study of the impact of disseminating arrest and conviction records, however, we submit that it would be a serious mistake to approach the problem addressed by S. 2008 as if there were a conflict between the interest in security against crime and the interest in the right to privacy. The wide dissemination of these records has not contributed to solving the problem of crime in America. It has helped to create the problem.

Millions of Americans are labelled by their records. As a consequence they are unable to obtain decent jobs or homes, insurance, credit, or admission to educational programs. The many surveys of the impact of personal records on people's lives point to a single inescapable conclusion: that arrest and conviction records often create social lepers who must exist as best they can on the fringes of society.

The dissemination of records places a series of obstacles in the path of persons who wish to enter society's mainstream and end the half-life of the world of crime. Is it any wonder, then, that recidivism rates should be so high? How can we seriously hope to reduce crime if we disseminate records which have the unintended effect of making it impossible for people to stop being criminals?

Law enforcement agencies may be able to come forward and describe instances in which crimes were prevented or criminals were apprehended because of the availability of records. Similarly, it may be possible to formulate examples of jobs which no sane person would want to be given to people with particular kinds of records. But we urge you not to permit such examples, even if they appear, to obscure the broad consequences of record dissemination practices. The United States disseminates arrest and conviction records more widely than any other country in the western world. We also have more crime. I believe there may be a cause and effect relationship.

When arrest records not followed by conviction are at issue, there are additional compelling reasons to prohibit dissemination. The most elementary premise underlying our commitment to due process of law is that a person is presumed innocent until proven guilty. That commitment is destroyed by criminal justice systems which punish persons not proven guilty through dissemination of their records. The impact of an arrest record is almost as severe as that of a conviction record in limiting opportunities for employment. Some people are started on the road to crime when they are arrested for things they did not do and labelled with arrest records.

No violation of the presumption of innocence is at issue when conviction records are disseminated. However, in addition to society's need to reabsorb convicted persons once they have been punished for their crimes in order to protect itself, there is a due process consideration in limiting punishments to those specified by the criminal law. If a legislature authorizes a judge to sentence a criminal to no more than a year in prison, that should be the limit of the punishment imposed. In practice, the dissemination of conviction records imposes life sentences regardless of the crime committed or the penalty specified by law.

The right to privacy is of vital significance. However, the concept of privacy is inadequate to describe the issues at stake in the measure you consider today.

The dissemination of arrest and conviction records causes millions of people to lead furtive existences. They either try to escape the criminal labels attached to them or, finding that struggle hopeless, conform to the labels. This country cannot afford to continue labelling an ever-increasing number of its citizens as criminals because it cannot afford to have so many criminals. We must seek ways to reduce the criminal population, and one way is to stop disseminating the records which label people as criminals and often cause them to act as criminals.

Let me now comment on some specific sections of S. 2008.

Section 103(c) excludes police blotters or other original books of entry from the ambit of this proposed legislation. We believe this is an unfortunate provision. Police blotters should be no more accessible than any other records.

Senator Ervin's original 1974 bill, S. 2963, did not contain any such exception. Its lack engendered criticism from some segments of the press. Many newspapers across the country routinely publish logs reporting all arrests. This information is obtained from police blotters. Section 103(c) permits this unfortunate practice. Since other provisions of S. 2008 would restrict alternate access to arrest records, employers, credit bureaus and other agencies seeking criminal justice data to deny people jobs and other benefits would get it from newspaper logs. In those communities where newspapers do not carry such logs, Section 103(c) would permit employers and credit bureaus to get arrest records directly from police blotters.

The press claim of a First Amendment right of access to police blotter data or arrest information generally seems to me without merit. I say this on behalf of the American Civil Liberties Union, an organization which has a record unmatched by anyone in defending freedom of the press.

The First Amendment absolutely protects the right of the press to publish whatever it chooses. In this way, the First Amendment allows the people to know what their government is doing. Moreover, even if the press should publish something government properly tries to conceal, it is dangerous to allow any government censorship. Inevitably, such power is abused. Therefore, prior restraint is absolutely forbidden and punishment subsequent to publication should be equally forbidden.

But the government is not obliged to reveal all of its actions to the press. It should not reveal those things which intrude on individual privacy. Does anyone argue that the government *must* reveal to the press:

1. Information prejudicial to a defendant in advance of a trial?
2. Details of individual tax returns?
3. Details about particular people gathered by the census bureau?
4. Details of medical records of individual persons treated in public hospitals?
5. Details of communications between individual soldiers and their military chaplains?
6. Details about individual home owners gathered by the F.H.A.?
7. Identities of drug addicts enrolled in publicly funded drug treatment programs?
8. Personnel employment files of public employees?
9. Anecdotal records of children attending public schools?
10. Case files of persons receiving publicly supported legal services?
11. Information about particular persons discovered through security checks of applicants for employment in defense industries?
12. Files on welfare recipients compiled by social workers?

In each instance, it might be possible to discover government abuses if the press were given access. The press and the public would learn about the legal services attorney who gave shoddy services to his client; the neglected public hospital patient, and the school child victimized by the halfbaked psychological judgments of his teacher. But in each instance, government properly attempts to conceal these records from the press and the general public. However great the abuses that might be revealed and curbed if these records were systematically disclosed to the press, those abuses would pale by comparison to the damage done individuals by revealing those government records.

Again, if the press gains access to any records, they should be publishable. Moreover, the subjects of these records should always have access to the records about themselves. If they consent, the government should release the records to the press. Their privacy is at issue, not the government's.

So it should be with arrest records. If the victim of an arrest consents, the arrest record should be made public. But it is sheer gall for segments of the press to insist, as they do, that to protect individuals from bad arrests, law enforcement agencies should disclose to the press arrest records even where the subject of the arrest

doesn't want the records disclosed. Moreover, the constitutional guarantee of due process of law should be read to forbid the government from imposing the punishment of arrest record dissemination on a person not convicted.

The due process violation was well stated by the United States Supreme Court in *Wisconsin v. Constantineau*, 400 U.S. 433 (1971).

In the *Constantineau* case, a Wisconsin police chief posted notices of excessive drinkers in liquor stores and bars. The Supreme Court said:

"Yet certainly when the State attaches 'a badge of infamy' to the citizen, due process comes into play. *Weiman* v. *Updegraff*, 344 U.S. 183, 191. [T]he right to be heard before being condemned to suffer grievous loss of any kind, even though it may not involve the stigma and hardships of a criminal conviction, is a principle basic to our society." *Anti Fascist Committee* v. *McGrath*, 341 U.S. 123, 168. (Frankfurter, J., concurring)

"Where a person's good name, reputation, honor or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential." 400 U.S. 433 (1971)

Identification of an arrested person to the press by a governmental agency, the police, certainly damages "a person's good name, reputation, honor, or integrity." The damage is as great whether the identification is from a police blotter reprinted in a newspaper or through a sign posted in a liquor store as in the *Constantineau* case.

Sections 201(b)(1)(D), (E), (F), and (G) are also troubling. The wording of these sections appears designed to provide for dissemination of nonconviction arrest record information to police officers engaged in stops and frisks. To understand the impact of these sections of the legislation, it is necessary to review the role of the National Crime Information Center in making stop and frisk a basic operating mode for American law enforcement.

The National Crime Information Center contains information on wanted persons, stolen property and, most relevant to Section 201, computerized criminal histories. Police officers who stop and frisk people or who stop them on traffic charges routinely radio identifications to terminals connected with N.C.I.C. More than 185,000 such transactions take place in an average day, or more than 70,000,000 a year. About three quarters of one percent of these transactions result in "hits." Ninety-nine and a quarter percent result in misses. These percentages suggest that police have no very good grounds for stopping people and making these checks on them. The number of "hits" scored is no better than could be achieved with purely random checks. Nevertheless, the total number of N.C.I.C. transactions is so large that even a three quarter of one percent "hit" rate is significant. It is law enforcement by serendipity. To maximize their small chances of getting "hits," police must maximize the number of times they stop people and check them out.

Section 201 (b)(1)(D) allows the dissemination of non-conviction arrest records in any case in which an individual has already been detained. This applies to all the people stopped and frisked and all the many millions of people stopped on traffic charges. Subsections (E), (F), and (G) seem designed to include those people on which N.C.I.C. checks are being made who have not yet been detained. The American Civil Liberties Union urges the deletion of subsections (D), (E), (F), and (G) of section 201 because they make arrest records not followed by conviction freely available to law enforcement agencies in the serendipitous effort to secure "hits" on the N.C.I.C. system.

The ACLU also urges the deletion of Section 203(h). In allowing public disclosure of arrest records not followed by convictions, although only at a time contemporaneous with the arrest, this provision resembles Section 103(c)(1) and our reasons for opposing that section apply with equal force to Section 203(h).

Even in the case of convictions, there are due process grounds for barring public officials from disseminating the records in the absence of consent from the subjects of the records. The punishment for any crime should be no more than that fixed in law. Record dissemination by law enforcement agencies provides an additional, often lifelong, punishment. Once again, if the press discovers the record, it should be free to publish it. And, if the individual consents, law enforcement agencies should make the record available to the press. But it violates due process for law enforcement agencies to disseminate conviction records to the press absent the individual's consent.

Finally, the American Civil Liberties Union urges deletion of section 204(b). This makes arrest records not followed by convictions freely available for federal employment purposes by executive order.

The federal government is the nation's largest employer. It should set an example to state and local governments and private employers of dedication to the presumption of innocence. This section permits the federal government, at the discretion of the executive, to rely on arrest records as a condition of employment. Section 204(b) runs counter to the spirit of this legislation and should be removed. If it is retained, at the very least, arrest records should be revealed only pursuant to statute and not also pursuant to executive order.

There is a growing awareness of the problem of punishment by record dissemination. Last year, the Congress took two major steps to deal with the problem. You adopted the Privacy Act of 1974 and the Family Education and and Privacy Act of 1974. In S. 2008, you confront the records most pervasively used to stigmatize people and deny them benefits. With the amendments I have suggested, I urge its adoption.

Britain has just adopted new legislation expunging conviction records of people sentenced up to 30 months in prison. And just last week, the New York State legislature adopted and sent to Governor Carey legislation authorizing the destruction of all arrest records not followed by convictions. Adoption of S. 2008 would ally the United States with the healthy trend to remove criminal record stigmas from citizens.

The problem of punishment by record dissemination was of no great significance when the due process clause was incorporated in the U.S. Constitution. At that time, the cure for an arrest or conviction record was to change one's name, move West, or simply assume an employer would never discover the record. Those methods of escaping records no longer work. Record dissemination is too efficient and pervasive. The punitive impact of arrest record dissemination has been increasing. When engaged in by public officials acting in the absence of consent from the victims of these records, it must now be regarded as a violation of due process of law. This legislation is urgently needed for protection for the right to due process and the right to privacy.

(Appended to this testimony is the June, 1975 edition of the American Civil Liberties Union's Privacy Report. It is mostly given over to a report on the uses of arrest records and current efforts to curb their dissemination.)

THE PRIVACY REPORT, JUNE 1975, NEW YORK, N.Y.

[Published by the American Civil Liberties Union Foundation]

ARREST RECORDS

You are arrested for robbery, tried, and acquitted; or

You are arrested for possession of marijuana, but the charges are dismissed; or

You are arrested with hundreds of others at a demonstration, but the courts later rule that the arrests were illegal; or

You are picked up for questioning about a theft in the neighborhood and detained at the police station overnight, but no formal charges are filed and you are released.

That should be the end of an unpleasant episode. But it may be just the beginning. Now you have an arrest record. Ignore it at your peril, for an arrest record can, and probably will, come back to haunt you.

THE ARREST RECORD TRAIL

When a person is "booked" at the police station, fingerprints and photographs are taken, and a form describing the arrest and the charge is filed. These are the raw materials of a "record." From the stationhouse the record trail follows a winding path, with many unexpected offshoots.

The path will most certainly lead to the FBI, the largest repository of arrest records in the country. The Bureau's Identification Division has the fingerprints of some 21 million people in its Criminal File. Information from the fingerprint card submitted by the "contributing agency"—ordinarily the agency making the arrest—is transferred to an identification record. If an individual is arrested more than once, the identification record becomes a kind of criminal history, called a rap sheet.

The FBI purports to be merely the passive custodian of identification information. It holds the contributing agency responsible for the data recorded in FBI files. If the contributor submits supplementary data, such as the disposition of the arrest charges, an acquittal, or the sentence imposed, these will be recorded; if the agency informs the FBI that certain entries are inaccurate, the Bureau says it will make the desired changes.

Arrest records are also distributed from the stationhouse to numerous municipal and regional record systems, which can exchange information among themselves and with centralized state systems. Some of these in turn may send information to another computerized criminal file maintained by the FBI, the National Crime Information Center (NCIC) Computerized Criminal History (CCH) system.

There are now over half a million criminal histories in NCIC. Each of these histories contains a full description of an individual and a record of his encounters with police, courts, and correctional agencies. CCH files are compiled from data submitted by computerized criminal information systems in four states (Florida, Illinois, Arizona, California), some federal agencies, and the FBI itself, which makes entries on federal offenders and on arrests in the District of Columbia. However, all states and numerous federal agencies are equipped to request CCH information *from* NCIC. The eventual goal, for the present bogged down in difficulties over money and privacy safeguards, is to bring all 50 states into the system as contributors as well as recipients.

The FBI's identification records are available to law enforcement and other kinds of governmental agencies, federal, state, and local. How information is used and disseminated is considered the responsibility of the recipients. Dissemination of CCH files is somewhat more restricted. Direct access is limited to criminal justice agencies (prospecutors, courts, corrections officials, and parole commissions as well as the police) and certain designated federal agencies, and these agencies must enter into written agreements with NCIC that preclude dissemination of CCH information for "unauthorized" purposes. The stated penalty for improper use or dissemination is expulsion from the system.

Arrest records are also in great demand by employers, particularly governmental employers. The FBI will supply information from its identification files to federal agencies, state civil service commissions and licensing boards, and federally chartered or insured banks for purposes other than law enforcement—primarily employment, bonding, and licensing. State criminal record systems will do the same for government or government-regulated employers and agencies in the state. In fact, a criminal record search is required by law in most states for a multitude of employment and licensing decisions, and the number of authorized recipients of criminal justice information in a state, both within and without the law enforcement community, may run to several thousands.

That is the *official* record trail. Federal and state laws appear to limit the dissemination of criminal records to specified users. But an absence of effective regulation, enforcement, and sanctions has allowed virtually unfettered dissemination of criminal records far beyond the "authorized" community: to private employers, landlords, credit reporting agencies, educational institutions, insurance companies, newspaper reporters, and all manner of social service agencies, both public and private. Almost anyone who cares to make the effort can get another person's criminal record.

Information can be bought from people who have authorized access. Information moves through "buddy" arrangements, as, for example, from policemen to retired policemen and their friends working in private industry. In many cities large employers have routine though "informal" access to police files. Reporters have told of the ease with which they are able to move through the record sections of some police departments. Political clout may be used to pry information out of timid agency employees.

Perhaps the worst damage is done when criminal records get into the hands of credit reporting agencies, for it is their business to sell information as widely as possible, to employers, insurance companies, banks, creditors, and landlords. The files of such agencies hold over 50 million investigative reports and several hundred million credit reports, and many of these may contain information on criminal records.

The arrest record trail, then, is not really a trail but a massive web. It has no end. As long as the record exists somewhere in the web, it can be reached and used.

### WHAT THE RECORDS CONTAIN

As there are no truly effective controls on the dissemination of arrest records, despite statutory strictures, it is then doubly important to control the information the records contain. The picture here is equally discouraging. The FBI stresses that it does not try to verify the accuracy of data contributed to it nor seek information on the disposition of the arrests it records. It is up to the agency making the arrest, therefore, to report to the FBI whether charges were dropped or prosecuted, and whether the defendant was acquitted or convicted. But often the

agency does not. And when the FBI disseminates records, it alerts recipients to contact the contributing agency to supply any missing information on the disposition of the arrest. But often they do not.

Brian N. was arrested twice; once he was tried and acquitted, the second time the charges were dismissed. A few years later he was hired by a firm that installed burglary alarms. His employer checked with the local police department, which checked with the FBI, which sent the records of Brian's arrests but not of the dispositions. The police gave that information to Brian's employer. Brian was fired.

Calvin L. deserted from the Marines in 1969, was arrested in 1973, and was undesirably discharged soon after. The desertion charges were never prosecuted. Later that year Dallas police stopped a car in which he was a passenger, ran an NCIC check, and arrested him on a "hold" for the military. He was released after four hours. Similar incidents occurred twice more over the next six months, one detention lasting 24 hours. Each time the NCIC check showed that Calvin was "wanted" by the military, but not that the charges had been dropped.

The same delegation of responsibility to contributing agencies for the completeness and accuracy of information is the practice of most state criminal justice record systems as well. But the contributing agencies have little incentive to submit follow-up information or correct errors. Threats of expulsion from the data system are useless—between 1962 and 1972, for instance, the FBI withdrew its identification services from only six small police departments—and indeed contradict the basic philosophy of an information system, which is to bring more participants into the exchange, not cut them off.

So, if you ever were arrested, there is a good chance that your record lies in at least one criminal justice information system, probably several, and has been or will be disseminated to any number of interested recipients. And there is a chance —enough of a chance to be worrisome—that your record is incomplete and inaccurate as well.

### WHY ARREST RECORDS MATTER

Arrest records matter for the simple reason that so many people believe they matter.

In connection with a homicide investigation, members of Milwaukee motorcycle gangs were picked up, booked, and photographed, but never charged. A document entitled "Known Members of Motor Cycle Gangs" with their pictures was compiled and handed out to police departments in the area. Since then many of these people have been stopped frequently by police, one person 18 times. In Washington, D.C., a young man was arrested and acquitted on a robbery charge. On at least three subsequent occasions the police showed his photograph in neighborhoods where crimes had been committed, and he and his family and friends were interrogated many times. Yet, but for his arrest record, there has never been any evidence to connect him with a crime.

The director of a local U.S. Employment Service office reported that the Service was able to place only 15% of applicants with records of convictions *or* arrests. An estimated 56% of all states, 55% of all counties, and 77% of all cities ask about arrest records on their civil service application forms. A study of New York area employment agencies showed that 75% would not accept for referral an applicant with an arrest record and no conviction. A California legislative committee found that applicants for post office jobs were automatically disqualified if they had arrest records. In a survey of 475 private employers in New York, 311 stated they would fire an employee if they discovered he or she had a criminal record. In another study 65 out of 75 employers said they would not consider an applicant arrested for assault even if the person had been acquitted. Most licensing and bonding procedures in every state either eliminate or treat adversely applicants with arrest records.

A person with an arrest record, then, is likely to command special interest from the law enforcement community, and very little interest in the employment market.

But does an arrest record really have any meaning? Often not, as these figures suggest:

In 1972 there were 8.7 million arrests in the United States, about 1.7 million of these for serious crimes such as homicide, rape, robbery, and assault. According to the FBI, about 20% of adults arrested for such serious crimes were not prosecuted, and of those prosecuted about 30% were not convicted. The percentages, of no prosecutions and no convictions were much higher for juvenile arrests and arrests for the 7 million less serious crimes.

The probability that a black urban male will be arrested at least once in his lifetime is estimated at 90%. For white urban males the figure is 60%; for all males, 47%.

A very large proportion of the arrests each year are illegal, or are made under statutes of dubious constitutionality, such as the loitering, vagrancy, and disorderly conduct laws that are widely used to sweep up the people who make street corner speeches, stand around idly on the sidewalks, talk back to policemen, play music in the parks, or look like homosexuals or hippies.

It is fairly easy to make an arrest; hundreds of people are arrested every day on misleading evidence, questionable evidence, or no evidence at all. It is quite something else to press charges that will stand up in court. It appears, however, that the average citizen's faith in the tenet "innocent until proven guilty" is not terribly strong. Many Americans apparently are not willing to wait for the verdict of a court, and believe that a person is sufficiently tainted by the arrest itself to justify suspicion and rejection. An arrest seems to mean that a person is guilty of *something*, and a failure to prosecute or even an acquittal seems to have little influence on that assumption.

The reasons for this attitude cannot be explored here. But anyone who has an arrest record must be forewarned that it is pervasive, and must take steps to protect himself against its destructive effects

## RELIEF: THE COURTS

The arrest record problem thus has two major components. The first is the uncontrolled dissemination of arrest records, often containing incomplete or inaccurate data. The second is the general public attribution of guilt to anyone who has an arrest record, and the translation of this attitude into such common abuses as police harassment and employment discrimination.

In recent years the courts have addressed some of these abuses and have offered various measures of relief to their victims, particularly in cases involving the maladministration of record systems or records of illegal arrests.

In *Gregory* v. *Litton Systems, Inc.*, 316 F. Supp. 401 (C.D. Cal., 1970), a federal district court heard the complaint of a black sheet-metal worker who had been arrested 14 times but never convicted. Litton had rescinded a job offer to Gregory when it learned of his arrest record. The court found that Litton's apparently racially-neutral inquiry into arrest records in practice operated to bar employment to black applicants in far greater proportion than to white applicants, and was not justified by any reasonable business purpose. The court ruled Litton's rejection of Gregory a violation of Title VII of the 1964 Civil Rights Act.

In *Menard* v. *Saxbe*, 498 F. 2d 1017 (D.C. Cir., 1974), the courts addressed the record-keeping practices of the FBI Identification Division. Menard had been arrested for suspicion of burglary, but never charged; in fact, it was never even established that any crime had been committed, for Menard had been picked up sitting on a park bench following a telephone complaint of a "prowler" in the neighborhood. Nonetheless, he was booked and fingerprinted, and held in custody for two days. The police routinely forwarded his fingerprint card to the FBI, and two days later sent the further notation "Released—Unable to connect with any felony or misdemeanor." The record was subsequently amended to designate a "detention" instead of an "arrest."

After the failure of negotiations with the FBI, the California Department of Justice, and the Los Angeles police—each of whom claimed it was "powerless" to remove the record on its own—Menard sued for expungement of his FBI file. Examining the administration of the FBI's criminal identification files, the district court found the operation "out of effective control." The appeals court noted the lack of procedures to assure accuracy and completeness of the records and to prevent improper use by agencies receiving FBI data. "The FBI cannot take the position that it is a mere passive recipient of records received from others, when it in fact energizes those records by maintaining a system of criminal files and disseminating the criminal records widely. . . ." Nor can the Bureau "turn aside its responsibility by claiming that it is powerless to act" unless a local police department formally requests removal of a record. Taking cognizance of the probable harm to Menard in continued retention of his "detention" record, the court ordered its removal from the FBI's criminal files.

Later that year the same court, in *Tarlton* v. *Saxbe*,—F.2d—, 43 U.S. Law Week 2191 (D.C. Cir., Oct. 22, 1974), addressed a second question: "to what extent, if any, does the FBI have a duty to take reasonable measures to safeguard the accuracy of information in its criminal files which is subject to dissemination?" This

case involved claims by a convicted offender that incomplete and inaccurate information in his FBI files had adversely influenced the court which sentenced him and the decision of a parole board to deny him parole. While not asserting that the FBI must actually guarantee the accuracy of its files or resolve conflicting allegations as to their accuracy, the court required "such reasonable care as the FBI is able to afford to avoid injury to innocent citizens through dissemination of inaccurate information."

Certainly the most sweeping expungement decision of all is *Sullivan* v. *Murphy*, 478 F. 2d 938 (D.C. Cir., 1973), cert. denied, 414 U.S. 880 (1974), a class action brought by the National Capitol Area CLU, in which the arrest records, fingerprints, and photographs of 13,000 persons illegally arrested in the 1971 antiwar "Mayday" demonstrations in Washington, D.C., were ordered retrieved and destroyed. Not only were the records to be recalled from all agencies, public and private, to which they had been disseminated, but the arrests themselves were to be deemed henceforth "detentions," so that the 13,000 plantiffs could, in the future, truthfully answer "no" if questioned whether they had ever been arrested.

Of special significance among recent arrest record decisions is the ruling of the Superior Court of the District of Columbia in *U.S.* v. *Hudson*, 43 U.S. Law Week 2377 (March 18, 1975), because it addressed the frequently heard argument that expungement of a record is tantamount to a denial of fact, a "rewriting of history." "It is clear," said the court, "that, when policy requires, our system of law renders existing documents and transactions null and void, permits the denial of facts, and adopts presumptions and legal fictions."

The *Hudson* decision and many others preceding it rest on a court's judgment that under the particular circumstances the harm to the individual's right of privacy outweighs any showing of a "compelling need" by the police or other law enforcement agency to retain the record. The majority of expungement cases to come before the courts so far have involved illegal arrests or questionable arrests followed by dismissal of charges, and abuses in the administrative practices of agencies collecting and disseminating arrest records. The definition of a "compelling law enforcement need" is yet to be judicially determined.

At the same time, the courts have not demanded a showing of actual harm caused by retention or dissemination of an arrest record. In *Menard*, for example, the court said that although the plaintiff "cannot point with mathematical certainty to the exact consequences of his criminal file," the disabilities and stigmas resulting from an arrest record were sufficiently well known and well documented to satisfy a showing of "cognizable legal injury."

Civil libertarians are pressing their view that the retention of an arrest record, where no conviction follows, is a violation of the Constitutional guarantee of equal protection—because people with arrest records are subjected to many of the same disabilities as those who have been convicted, whereas they are entitled to be treated exactly like all other people who have never been convicted of a crime. It is also argued that such retention is cruel and unusual punishment, a subjection to harsh penalties without due process of law, a violation of the Constitutional presumption of innocence, and a facilitation of police surveillance constituting an invasion of the right of privacy.

All these arguments are raised in current ACLU litigation in *Doe* v. *Kelley*, Civ. Action No. 74-1394 (D.D.C.). In 1947 "Jane Doe" married a man who, four years later, was arrested by the FBI and convicted for transporting stolen goods across a state line. Jane Doe was arrested too, but as she had known nothing of her husband's crime, the charges against her were dismissed.

However, Jane Doe still has an arrest record in the FBI's criminal identification files.

Ms. Doe's marriage was annulled in 1954. She remarried and went on to a successful career in public education, as a school superintendent and principal, author of articles in professional journals, and educational consultant to several governors.

Now Ms. Doe is trying to erase the shadow of her 24-year-old FBI record. Her career, she asserts, has constantly been plagued by the fear that her record will be disseminated or exposed by the FBI, and she has passed up numerous opportunities for professional advancement for fear that her record will be discovered. Such a discovery would, at the very least, deprive her of a promotion, and might actually lead to her dismissal.

This case is now in the courts, but it appears that an agreement by the FBI to destroy Ms. Doe's record and recall it from any other agencies to which it has been disseminated may be imminent.

RELIEF: THE ADMINISTRATIVE CHANGES

Though courts have increasingly shown a willingness to deal with arrest record abuses, the relief available through the judicial process is very limited. The most obvious limitation is that relief is granted only to the parties to the case. Not everyone who is victimized can go to court. Dale Menard's victory did not create a revolution in FBI record-keeping practices, nor will the expungement of Jane Doe's file mean the destruction of thousands of other stale records. The *Gregory* decision did not stop other employers from inquiring into arrest records.

On the other hand, some small changes have taken place. In 1973 the FBI published a procedure whereby people who have records in its Identification Division may obtain a copy by submitting a request (with name, date and place of birth, a set of fingerprints, and $5) to FBI, Identification Division, Washington, D.C. 20537. If the person believes the file is incomplete or inaccurate, he or she is told to contact the agency which contributed the record. The FBI will make any changes requested by that agency.

In 1974 the FBI announced a new policy governing its dissemination of arrest records to banks and state and local agencies not involved in law enforcement. Such records will not be supplied if the arrest is over a year old unless information concerning disposition is included. Dissemination to law enforcement agencies will proceed as before, however.

RELIEF: THE STATE LEGISLATURES

A number of states have procedures allowing for expungement of arrest records. Relief is usually limited to persons charged with certain categories of crimes, and often takes the form of "sealing" rather than erasure. This means that the record remains physically in existence, but subject to various restrictions on access. Some states also have laws forbidding employers to ask about certain kinds of arrest records.

Connecticut, for example, has a statute which allows a person found not guilty, or against whom charges were dropped or not prosecuted, to have all records, fingerprints, and photos returned within 60 days following application to a clerk of the court—*except* a person previously convicted of a crime.

Maine's statute, in addition to expungement, provides that an acquittal or dismissal "shall mean that the person shall, for all purposes, be considered as never having been arrested," and that no employer or other person may use that arrest to his detriment. However, it does not forbid employers to inquire. Illinois forbids employers to inquire in writing, but not verbally.

Massachusetts will seal arrest records and some conviction records for a variety of crimes. In some situations the person must petition a court, in others, the state Commissioner of Probation. The law allows an employer to ask about arrests but also requires him to inform applicants that they may answer "no record" with respect to any sealed record.

Florida's expungement law applies only to arrest records of persons not previously convicted of a crime, and even then "non-public" records may be maintained by the Department of Law Enforcement, available for future use if that person should be the subject of a criminal investigation.

Aside from the fact that relief is limited, and often hedged about with exceptions and qualifications, many of these laws also require that the person who has been arrested initiate the expungement or sealing process, yet do not oblige any law enforcement or court officer to notify the person of his rights.

In many jurisdictions the laws have not been working well even within their narrowly drawn terms. In Connecticut, for example, some officials have created a separate file for "erased" records, while others have simply stamped "erased" over the records. The state police have used liquid paper to blot out the sections of records which are supposed to be expunged.

An analysis by the Massachusetts CLU of the operation of the sealing laws in that state points up many of the problems facing those who try to wipe out their arrest records.

First, because the records are sealed rather than expunged, they are still available for legally authorized—and unauthorized—purposes. Thus, the records may be opened in connection with sentencing for subsequent convictions, and are available for inspection by criminal justice agencies which, by law, are forbidden to hire ex-convicts.

Second, relief is by no means automatic. Many records are sealed only at the discretion of the court. Moreover, relief is available only to people who know

about the law, with the result that very few of those eligible ever get their records sealed. Ironically, automation, so often blamed for the abuses attributed to record-keeping systems, could actually facilitate the operation of an expungement procedure without any burden upon the record subject, or upon the clerical staff who handle the records.

Third—and this is a crucial flaw common to almost all expungement and sealing procedures—the law does not require a thorough search of all the files to which the record may have been sent. We have seen how widely arrest records are routinely disseminated. It is not enough to stipulate expungement in some central record repository, when the record may still be freely available in dozens of other data systems around the state, even across the country.

The Massachusetts CLU also found "a prevailing pattern of non-compliance" by employers with the requirement of a notice on application forms that questions concerning criminal records may be answered "no" with respect to sealed records. Of the employers surveyed, nearly half of the governmental agencies inquired about criminal records but did not supply the notice. Nearly 75% of the private employers did the same. Nor does the law prevent an employer from obtaining information about sealed records from a source other than the applicant, such as a credit reporting bureau.

But there are occasional pleasant surprises. One instance: The Maine Civil Liberties Union reports that clerks of the court in Cumberland County automatically issue expungement notices to all police agencies whenever there is a dismissal or acquittal, regardless of whether the defendant requests it or is even aware that the law exists. And this is in spite of the fact that the law appears to require the defendant to initiate the expungement.

### RELIEF: CONGRESS

Long-awaited Congressional action on criminal justice records now seems unlikely to afford an effective solution to the arrest records problem, even if a bill is passed this session—which is questionable.

In the 93rd Congress, Senator Sam Ervin was the principal sponsor of a bill that would have placed some controls on the dissemination and uses of arrest and conviction records, and provided for expungement or sealing of certain kinds of records. An amended (and weakened) version of this bill, S. 1427, now sponsored by Senator John Tunney, has been introduced into the 94th Congress, along with an Administration bill, S. 1428, and companion bills in the House, H.R. 62 and H.R. 61. But the Tunney bill would only seal or expunge arrest records two years after the arrest, if there has been no conviction and no prosecution is pending, and access to sealed records would remain available to criminal justice agencies for a variety of law enforcement and other purposes. If adopted in anything like its present form, this legislation cannot be considered a remedy equal to the dimensions of the problem, though it may help to curb some of the most flagrant abuses of record maintenance and dissemination.

(The Privacy Act of 1974, you will recall, exempts most criminal justice record systems, although it does require that the information maintained in these systems be kept "timely" and "accurate." See March *Privacy Report.*)

### RELIEF: A CHECKLIST

If you ever were arrested, you should write the FBI Identification Division for a copy of your record. If you note any inaccuracies, in particular the absence of disposition information, ask the agency that arrested you to request the FBI to correct the record.

Then find out what expungement or sealing procedures are available in your state and follow through on every possibility. Remember to demand that your record be recalled from every agency that received it.

Finally, you may want to consider going to court if (1) you believe the arrest was illegal or unconstitutional; (2) the record concerns a "detention" rather than an arrest; (3) you believe the record has been disseminated to unauthorized persons; or (4) the record contains false or incomplete data that may cause you damage.

## In the Courts

### SEARCHES

A federal district court ruled that the use of specially trained dogs to sniff out concealed marijuana whose odor would be undetectable to humans is a violation

of a person's "reasonable expectation of privacy," and is therefore impermissible in the absence of a warrant satisfying Fourth Amendment standards of probable cause. *U.S.* v. *Solis*, 43 U.S.L.W. 2425 (C.D. Cal., March 27, 1975).

However, the Ninth Circuit Court of Appeals said that a parole officer may search a parolee's home without meeting Fourth Amendment warrant and probable cause requirements if the search is based on a suspicion arising from what the officer knows about the parolee's attitude and behavior. The rehabilitative purposes of the parole system give the officer a unique interest in invading a parolee's privacy, in the majority view. But the dissenters argued that the rehabilitative purposes of parole "would be advanced, not impeded, by a warrant requirement." *Latta* v. *Fitzharris*, 43 U.S.L.W. 2460 (9th Cir., April 15, 1975).

#### VOICEPRINTS

A Massachusetts state court has accepted expert testimony on spectrographic analysis—the voiceprint—as evidence in a criminal trial, ruling that the voiceprint has met the test of "general acceptance in the scientific community." *Commonwealth* v. *Lykus*, 43 U.S.L.W. 2434 (Mass.Sup.Jud.Ct., March 27, 1975).

#### EAVESDROPPING

A Michigan court found that the admission of police testimony concerning the identity of the defendant, based on information monitored during an illicit drug sale by means of a concealed radio taped to an informer's chest, violated the state constitution's provision against unreasonable searches and seizures. The court declared itself "persuaded by the logic" of the dissenting opinion by Supreme Court Justice Harlen in *U.S.* v. *White*, 401 U.S. 745 (1971), which had argued that one's expectation of privacy should not be diminished by the possibility that communications directed to particular persons will simultaneously be intercepted by a third party, unless pursuant to a valid search warrant. The Michigan court did "not condemn the exercise of participant monitoring by law enforcement personnel. However, when circumstances justify the use of this surveillance technique, the resulting search and seizure must be conducted in full compliance with the warrant requirement to be properly admitted at trial." *People of Michigan* v. *Beavers*, 43 U.S.L.W. 2446 (Mich.Sup.Ct., April 7, 1975).

### In the Agencies

#### FBI DOSSIERS

Many people making Freedom of Information Act requests for their FBI intelligence dossiers have received a form letter from Director Clarence Kelley asking for complete name, date and place of birth, prior addresses, employments, and "additional identifying data."

ACLU has been advising people to supply the first two items and their current permanent address, and one earlier permanent address if they have moved within the last year. To supply all of the data requested is really to submit a self-compiled, ready-made dossier with many bits of information the FBI would be happy to have. On the other hand, the FBI has a duty not to release information without some assurance of the recipient's identity. The ACLU urges a "rule of reason"; obviously, if your name is John Smith, or if you have moved half a dozen times in the last year, you may need to identify yourself with some particularity.

Senator Thurmond. Again I just want to reiterate—and this is a big question for us today, it is a question before the American public—who are we going to put first, the individual or the public, your family and everybody's family, or one individual, where there is a conflict? I think we have got to realize that. And I don't think we should do anything that is going to obstruct the enforcement of the laws, whether Federal or State, or impede the necessary operation of the agencies that are trying to protect the public.

Some people have tried to prejudice the public against the police departments and other law enforcement agencies as well as the military. Well, their function is to protect the public. They are created by government and are created by you and me and others engaged in government. These organizations are not created to harass, and if

they do harass, there are laws whereby they can be punished. They can be sued, and they can be prosecuted criminally. But their job is to protect the public. And what protection do we have from criminals if we don't have a police department? And on a national basis what protection do we have from our enemies if we don't have a military?

Therefore, I would hope that this subcommittee would be very careful not to do anything that is going to result in a situation where an individual will have rights above those of the public. I think that would be very dangerous.

Again, I want to emphasize that I think it is important, however, to protect the rights of the States. If there has been any action taken by the Federal Government that does not preserve the rights of the States, then that can be considered in court. The rights of the States are protected under the Constitution. If the Federal Government is taking some action, as Mr. Neier referred to, that is in violation of a State law, that can be taken up in court. We don't have to pass a Federal law for everything that comes along.

I am getting sick and tired of growing Federal intrusion into people's lives and into the rights of the States. When I go back to my State of South Carolina the biggest complaint I hear is more Federal intrusion, more Federal interference.

People are getting tired of it. We should stop and think and carefully consider and appraise just what we want to accomplish without bringing about more Federal intrusion that can bring inconvenience and even tyranny into people's lives.

Senator TUNNEY. Senator, there is one point I would like to make. Although the Deputy Attorney General referred to S. 1428, which was the administration's bill, as representing an avoidance of the imposition that restricted Federal control to its operations as to the State and criminal justice agencies, and whereas he characterized S. 2008, the committee bill, as establishing that kind of intrusion, I would hope that you would look at those two bills yourself.

It is certainly my position that right now you have a very substantial Federal intrusion—without any legislation—on the State and local government by the operation of the NCIC and by the FBI. The design of S. 2008 is to give to the State and to the local law enforcement agencies a greater voice in the management and the use of this computer technology for the storing of records and the dissemination of records. Mr. Tyler says that it is exactly the opposite, but I would ask you to make your own individual judgment on it. One of the things I certainly am trying to do in the legislation that I have authored is to give to State and local governments a voice in a system that has a national application, that already is being used without any Federal legislation such as the one in the bill before us providing guidelines.

I think that the Justice Department, through Mr. Tyler, is wrong when it suggests that we are trying to create a greater intrusion. We are trying to create a lesser intrusion, if you want to know the truth. But I ask for your own individual judgment of it when you have a chance to read both bills with a degree of specificity.

Senator THURMOND. Thank you very much.

I notice he makes a statement that S. 2008 establishes a Federal commission to oversee administration and enforcement of the legislation's provisions and to issue binding Federal regulations and inter-

pretations. I think we had better take a look at this commission, because we don't want to give the Federal Government powers——

Senator TUNNEY. The commission is made up primarily of State and local law enforcement officials. The reason we did it that way was that we wanted State and local law enforcement officials to establish policy for the use of this computer technology to store and disseminate records. As it is now, the Director of the FBI has that power, and he is using that power. He has an Advisory Committee, but it has no power to impose its will on him if he chooses to ignore it. What we are attempting by the commission to do is to give to the State and local law enforcement agencies a greater voice, a dominant voice, as to how these systems were going to be established. Now, as I say, the Director of the FBI has that power all by himself, and most State and local law enforcement officials that I have talked to don't like it at all.

They want a commission where they have the dominant voice, and that is what we give them with our commission, the dominant voice.

Senator THURMOND. Perhaps, we could do that without setting up a Federal commission with the power to issue binding regulations and procedures. Anything that can be done to keep this matter in the hands of the States is very commendable. Maybe we can work out a bill that will accomplish the desired objections without this Federal power.

Police power has always been considered a responsibility of each State. I was Governor of a State, and was responsible, as Governor, as the chief executive officer, to see that the law was enforced in that State. The State included a number of counties and cities, and we depended upon the sheriffs in the counties and the police departments in the cities to enforce the law. The Governor had the right to remove a sheriff, and the power to enforce it. I don't think the Federal Government ought to take any step to intervene in that power, because after all, we have got 51 sovereign governments in this country. We have got 50 States, and the State governments have got complete power for law enforcement in those States. I don't want to see that right infringed upon by the Federal Government, and I am sure you don't.

Senator TUNNEY. No, I don't.

Senator THURMOND. If any Federal agency is pursuing any course to infringe upon that right of the States, the agency may have to be stopped. At the same time, I do think possibly, where it is a great inconvenience to the different States, that we should have someplace where records are kept and could be made available. The records should only be available when requested by proper authorities to help them, and not available to enable them to impose their will. A State cannot keep a record of every criminal in the United States, and maybe the FBI is a propor agency to keep those records which would help the State when the proper authorities request that information. However, this is a delicate situation.

To reiterate, I am continuously getting complaints about Federal intervention, Federal intrusion. By a review of the other areas in which Federal legislation has been enacted, it appears like the Federal Government wants to run everything. I think the Federal Government ought to be the restricted, limited government that was provided in the Constitution. I think we have gone beyond that in so many ways

and the quicker we can reverse that trend, the better for the people and the better for the Federal and State Governments.

Thank you very much.

Senator TUNNEY. Thank you, Senator.

The live quorum just sounded. By the rules of the Senate, we will have to end this hearing.

Mr. NEIER. Thank you very much.

Senator TUNNEY. Thank you very much.

[Whereupon at 10:35 a.m., the subcommittee adjourned, subject to the call of the Chair.]

# APPENDIX

## ADDITIONAL STATEMENTS

### Prepared Statement by the Alarm Industry Committee for Combating Crime Concerning Proposed Criminal Justice Information Legislation

Prior proposed legislation, H.R. 61 and 62 and S. 1428, as well as the pending bills, S. 2008 and H.R. 8227, have not reflected the need for relevant criminal record conviction information by private security companies.

The Alarm Industry Committee for Combating Crime is an *ad hoc* committee composed of the following companies and organizations:

Central Station Electrical Protection Association; National Burglar and Fire Alarm Association; American District Telegraph Co.; Westinghouse Security Systems; Honeywell Protection Services; Holmes Protection, Inc., Wells Fargo Alarm Services; and Diebold, Inc.

AICCC represents a broad segment of businesses providing burglar and hold-up alarm services, including central station service, alarm system installation and maintenance, alarm system monitoring, guard response to alarm signals, and the manufacture of alarm systems and components for businesses, financial institutions, residences, and federal, state and local premises.

Certain employees of private security companies, including alarm companies, protect the property and lives not only of private citizens and of businesses vital to our national economy but also protect military installations, government buildings, hospitals and, in some instances, criminal justice agencies. Private security employers have a legitimate need to know if any of their employees have been convicted of crimes which reflect on their fitness to protect the property and lives of others. If private security employers are not given access to relevant criminal conviction record information, criminal elements could infiltrate private security companies, endangering lives and property and subjecting private security companies to law suits if employees with conviction records are involved in committing crimes against the persons or property they are employed to protect.

The proposed compromise legislation, S. 2008 and H.R. 8227, introduced in this session of Congress, provides only—in Section 203—

> "(a) Except as otherwise provided by this Act conviction record information may be made available for purposes other than the administration of criminal justice only if expressly authorized by Federal or State statute."

If this legislation becomes law, private security employers would be required to seek and obtain legislation in all 50 states in order to obtain the criminal conviction record information necessary to assure that their employees and agents are not criminals. This is an onerous and unfair burden to impose upon this industry and presents a serious threat to the safety of individuals and the security of governmental agencies. At a time when we are devoting major resources in an effort to reduce crime, such legislation would have the effect of encouraging it by offering criminals an easy target.

In a study by the Rand Corporation released by the Department of Justice in 1971, statistics reflected that there are as many or more persons employed in the private sector as guards, watchmen or alarm response personnel as in the public law enforcement sector. In some cases, private security personnel are also armed. Most central station companies, for example, send armed guards to respond to burglar and hold-up alarm signals, as well as notifying local law enforcement authorities.

The Law Enforcement Assistance Administration of the Department of Justice, acting under the Federal Advisory Committee Act, has established a Private Security Advisory Council, which includes among its members persons engaged

in the business of providing private guards and watchmen, armored car service, burglar and hold-up alarm protection and private investigative services. Also included on this advisory committee are consumers of such services and public law enforcement officials.

The Private Security Advisory Council has been developing model legislation designed to provide for fair and reasonable licensing of businesses and persons engaged in private security activities, and an essential ingredient of such model legislation are provisions for criminal conviction investigations of persons entering the private security business and their employees. It may be some time before the work of the Private Security Advisory Council is finished and the material distributed throughout the states for consideration by their legislatures.

Among the recommendations of the Private Security Advisory Council (PSAC) to LEAA was a statement, unanimously passed, which supported the right and the need of private security employers to have relevant criminal conviction information before hiring employees. A copy of the minutes of the PSAC meeting, which includes PSAC's recommended position statement, is attached.

The opinion of that body as reflected in minutes of its meeting on the issue is that persons entering the private security business and employees charged with protecting premises and persons—or having confidential information which could be used to defeat or compromise a security system—must be subject to a relevant criminal conviction record check before they are permitted to engage in the business or to be employed by such business. AICCC recognizes the need to control the dissemination of criminal justice information, but the right of persons to be secure and safe in their homes and business is an equally vital one and must be given proper consideration.

The position of AICCC is that it is not sufficient for private security employers merely to obtain a license from a licensing authority before hiring an employee. There are many jurisdictions in which no licensing authorities exist and, under the various legislative proposals, certain existing local licensing authorities would not be able to obtain criminal conviction information unless further legislation is enacted by the states.

We attach herewith a copy of a resolution passed by the National Burglar and Fire Alarm Association which reflects the position of this Committee.

Respectfully submitted,

MORISON, MURPHY, ABRAMS & HADDOCK
*Counsel for AICCC,*
By BERNARD M. BEERMAN.

NATIONAL BURGLAR AND FIRE ALARM ASSOCIATION, INC.,
*Washington, D.C., July 9, 1975.*

BERNARD M. BEERMAN, Esquire,
*Legal Counsel, Alarm Industry Committee for Combating Crime, Morison, Murphy, Abrams & Haddock, Washington, D.C.*

DEAR MR. BEERMAN: Based on the very serious concern of the alarm industry over any legislation which might preclude the obtaining of necessary criminal justice information such as conviction data on our employees and applicants, a Resolution was unanimously adopted by the National Burglar & Fire Alarm Association, which reads as follows:

"Be it resolved that the National Burglar & Fire Alarm Association strongly believes that a legitimate right and need exists for private security employers, such as burglar alarm installation and service companies, to have access to criminal conviction data of private security employees and applicants which is contained in criminal justice information systems. It is also the belief of this association that citizens have a right to be free from unwarranted and unnecessary intrusions on their privacy, and the development of a national criminal justice information system without security and privacy control increases the danger of such intrusion.

Therefore, the National Burglar & Fire Alarm Association supports and encourages the concept of protection of privacy and security and criminal justice information systems provided such systems legally recognize and provide for private security employer access to conviction data of private security employees and applicants."

If we can be of any assistance whatsoever in your preparation for either oral or written testimony, please let me know.

Sincerely,

GARIS F. DISTELHORST, *Executive Director.*

[Excerpt from the LEAA report on the Dec. 11–13, 1974, meeting of the Private Security Advisory Council]

5. Security and Privacy

At the September meeting, the PSAC directed the staff to research and prepare a position for the Council on the issue of security and privacy. Mr. Crowley presented a draft position statement to the Council.

In the discussion that followed, several members felt that the position statement which called for private security employer access to criminal conviction data did not go far enough and that the private security industry had a need for access to criminal data on a broader scale. It was suggested that security personnel, conducting criminal investigations for a corporation should be able to request data on all employees under investigation. Some suggested that there should be access to data on all employees or applicants where the individual was to fill a sensitive position. The failure to achieve consensus led to the appointment of an Ad Hoc Committee chaired by Chief Derning to meet separately and report back to the full Council with a new statement.

Chief Derning subsequently met with the Ad Hoc Committee and reported back to the Council that his Committee recommended the following position statement:

"The National Private Security Advisory Council strongly believes that a legitimate right and need exists for private security employers to have access to criminal conviction data of private security employees and applicants which is contained in criminal justice information systems. It is also the belief of this Council that citizens have a right to be free from unwarranted and unnecessary intrusions upon their privacy and that the development of national criminal justice information systems without security and privacy controls increases the danger of such intrusion.

Therefore, the National Private Security Advisory Council supports and encourages the concept of protection of privacy and security in criminal justice information systems provided such systems legally recognize and provide for private security employer access to conviction data on private security employees and applicants."

A motion was made that the Council adopt the recommended position statement and, after discussion, the motion was passed unanimously.

---

Prepared Statement of the International Association of Chiefs of Police

The International Association of Chiefs of Police is pleased to have this opportunity to elaborate on our views regarding Senate Bill 2008. The IACP is the world's leading association of police executives with more than 10,000 members representing every state in the Union, as well as 60 other nations. Throughout our 82 years of existence, we have consistently pressed for the upgrading and professionalization of police services. Especially during the last decade, we have undertaken or supervised a wide range of research and training programs. The basic aims of the IACP are to foster police cooperation and the exchange of information and experience among police administrators throughout the world; to bring about recruitment and training of qualified persons; and to encourage adherence of all police officers to high professional standards of performance and conduct. Since we have such a broad constituency, we feel we can truly speak for the needs and concerns of the entire law enforcement community.

The vast majority of police departments are opposed to any form of legislation similar to Senate Bill 2008. The members of IACP are aware that the American public has become concerned about the power which may be improperly wielded by governmental agencies straying beyond the bounds of their proper missions. Indeed, we in the law enforcement community have long been aware of the fact that intensive intelligence and investigative operations and the maintenance, use, and dissemination of criminal justice information present potential threats to individual rights. It is because of this very awareness that law enforcement agencies have severely restricted access to files and have instituted strict security measures with regard to all forms of criminal justice information, intelligence information, and investigative information.

Although a few criminal justice agencies have not established strict procedures and may have overestimated the needs of law enforcement in relation to individual rights, the existence of these few situations does not mandate Federal legislation imposing stringent standards on all state and local agencies. Indeed, despite the recent public focus on privacy and intelligence operations, there have been few

substantiated reports of violations committed by state and local law enforcement agencies. Passage of Federal legislation at the present time would constitute a failure by the Federal government to recognize that even before public attention was focused on the right of privacy, criminal justice officials have taken actions deemed necessary to protect individual rights of privacy.

The Federal government has consistently recognized, and should continue to recognize, the right and ability of the states to legislate in the field of law enforcement. One of the cornerstones of our American democracy has been the absence of national control over the police. Throughout our 200 years of existence, we as a nation have opposed Federal control over state and local police, no matter how well-intentioned the purposes motivating the Federal legislation. This tradition of the autonomy of state and local police has arisen from a recognition of the people's need to have control over the police exercised by those governmental bodies closest to them—the states and the localities. By taking yet another step toward national control over the police, we are actually further endangering individual rights.

Because of its comprehensive scope, S. 2008 underutilizes the ability of the states to fashion their own law enforcement standards and procedures. The fact that few states have enacted comprehensive statutes addressing the criminal justice information and intelligence areas should not lead to a conclusion that the Federal government needs to legislate. Few states have addressed all the ramifications of this problem, because it is only recently that the public and the legislators have come to realize the scope of problems presented in the privacy field. The Federal government, likewise, has only recently given attention to this field.

A number of states, such as Massachusetts, New York, and Florida, have recently enacted legislation controlling intrastate exchanges of information. Many other states are now developing or considering similar legislation. These new state laws, along with the Project SEARCH Model Statute, can spur other states to examine the problems of privacy and criminal justice information. If comprehensive Federal legislation is not enacted, each state will retain the right to decide how to balance the competing interests and will be able to fashion legislation addressing particular needs.

Essentially, we believe that S. 2008 unnecessarily imposes upon state and local agencies detailed standards dictated by the Federal government. S. 2008 represents an attempt to establish through Federal legislation certain uniform standards and procedures for the access, use and dissemination of all forms of criminal justice information. The Bill is comprehensive in scope and requires state and local agencies to adopt certain rules or regulations even with regard to solely intrastate exchanges of information. S. 2008 attempts to specifically limit the uses of criminal justice information, and, through its establishment of a Commission with extensive rulemaking and enforcement powers, it could remove from the states and the individual criminal justice agencies the ability to exercise discretion in a large number of areas.

Federal legislation like S. 2008 will stifle creativity, since it fails to take advantage of the ability of the states to fashion protections and remedies best suited to their individualized needs. A fatal flaw of S. 2008 is that it basically fails to recognize that procedures established for an enormous and complex system, such as NCIC, are not necessarily the best procedures to be applied to a small police department's file system. No one is now able to foresee all the variables which may arise regarding the future need for, and methods of access to, criminal justice information. The rapidity with which computer technology has recently advanced attests to this fact. Enactment at this time of a Bill which sets forth detailed standards aimed at every type of criminal justice information system could lock agencies into methods which are neither the most effective nor the most secure; it could have unpredictable side effects preventing experimentation and seriously hampering law enforcement efforts.

We believe that if any Federal legislation is enacted at this time it should not remove from the states the duty and power to fashion particular standards and procedures to protect individual rights. A better approach to legislation would be to differentiate between systems involving only state and local agencies, and those addressing Federal or joint state-Federal systems, with Federal legislation only as to the latter.

Proper legislation should not dictate the particular standards or procedures to be adopted by systems maintained or used solely by state and local agencies. Rather, it should confine itself to the enunciation of certain general goals to be accomplished by state and local agencies. The goals stated in the Act should be

general; they should leave to the discretion of the states the decision as to where to strike the balance between the rights of privacy and free press, the needs of law enforcement, and the desire of the public safety. Such goals should include: (1) specification of limits on the dissemination, exchange, and use of criminal justice information, intelligence information and investigative information; (2) establishment of procedures assuring the security and accuracy of criminal justice information, intelligence information and investigative information; (3) establishment of provisions guaranteeing individuals the right to challenge the accuracy of criminal justice information maintained on them; (4) provision of appropriate sanctions for non-compliance with announced standards; and (5) goverance by formal written agreement of interstate information exchanges. No Federal agency or national commission should be given rulemaking or enforcement powers with regard to systems of a purely local character; although the Federal government or a national commission might aid the states by studying problems arising in this field, by drafting model statutes, rules and regulations, and by presenting these models to the various states and criminal justice agencies for consideration. The states and criminal justice agencies would not be forced to adopt these models; rather, they could fashion whatever standards and procedures they deemed best suited to meet the general goals.

The problems posed with respect to state-Federal, local-Federal or purely Federal information exchanges are somewhat different, since the lack of uniformity has serious effects at this level. This lack of coordination is compounded by the rulemaking powers of various Federal agencies. At present, state and local agencies have no ability to control the standards and policies of central Federal criminal justice information systems, even though the state and local agencies are the principal users of central systems like NCIC. If there is to be Federal legislation, it could protect state and local agencies utilizing central Federal information systems by setting certain minimum standards to be followed by Federal criminal justice information systems. Legislation should provide for only that rulemaking power deemed necessary to' apply these standards to local-Federal, state-Federal or purely Federal exchanges of criminal justice information. In order to guard against conflict with the right of states to regulate their own systems, this rulemaking power should not be extended to allow for nationl control over the procedures of state and local criminal justice agencies with regard to any information not obtained from a Federal system.

Unfortunately S. 2008 is not only an intrusion by the Federal government into a field traditionally left to the states; it is a restrictive measure which would seriously curtail the ability of law enforcement agencies to protect the public. Discussions relating to criminal justice information and the right to privacy have focused on the need to balance three key interests: (1) the rights of privacy of individual citizens; (2) the necessity for law enforcement to utilize the tools needed to detect criminals; and (3) the right of the public and press to be informed. In our opinion, the balancing of these three key interests has been improperly applied in S. 2008. One key societal interest not directly addressed is the right and need of the public to protection—to be free from crime and the fear of crime. Focusing on this interest, as well as the other three, leads one analyzing S. 2008 to realize that the effect of the severe restrictions imposed on legitimate activities and procedures of law enforcement agencies will be an unnecessary reduction in the protection afforded the public. Crime is still a major threat to the American public, and we feel certain that the Congress would want to be particularly cognizant of the effects of restrictive legislation like this Bill upon the ability of law enforcement to fight crime in America.

If the restrictions imposed in this Bill result in the inability of police to detect murderers, rapists or saboteurs, with the result that those persons remain free to continually commit crimes of violence; the rights of Americans would be unnecessarily endangered. Unfortunately, the result of this Bill as now written, would be that many violent criminals would remain free. To grant such a benefit to organized crime and criminals is much too heavy a price for society to pay.

We have pointed out two key reasons why we believe the Bill is unsound: The dangers arising from increased Federal control over law enforcement; and the increased exposure of the American public to crime, due to the curtailment of law enforcement activities. These conclusions are based upon a careful analysis of the provisions of S. 2008; specific criticisms of the most significant problems follow.

Section 201(b)(1)(E) would severely restrict access by law enforcement agencies to arrest record information, by allowing dissemination for investigative purposes only after the requester had met the "*Terry* test." Although we recognize the need to prevent arrest or nonconviction information alone from being used to

determine an individual's probability of guilt, we would like to point out the restrictive and dangerous effects of the statutory language employed in section 201. The "*Terry* test" set out in section 201(b)(1)(E) is misstated, misapplied and out of context. The drafters of this Bill have used as a statement of the Reasonable Suspicion Test language that was only cited in *Terry v. Ohio* as a general statement of Fourth Amendment protections and was, therefore, only dicta. Moreover, the language itself has been changed by the drafters of the Bill. Although the drafters have indicated that the language employed outlines a *Terry* Reasonable Suspicion Test, the standard actually approaches probable cause. *Terry* indicated that the determination of what protections are afforded by the Fourth Amendment depends upon a balancing test.

The greater the extent to which the police actions intrude upon a suspect's Fourth Amendment rights, the harder it will be to meet the test. Thus, arrest, an extreme intrusion could only be justified by probable cause. On the other hand, a mild intrusion, such as a records check, should require a minimal quantum of facts and inferences. S. 2008, by tying the language of the "*Terry* test" to the phrase, "conclusion that the individual has committed or is about to commit a crime", a phrase which was not employed in *Terry*, raises the general Fourth Amendment standard expressed in *Terry* almost to probable cause.

Furthermore, use of a Fourth Amendment test to restrict access to criminal justice records is a total break with past case law. The courts have been consistently aware of their role as protectors of individuals' Constitutional rights, and they have fashioned various forms of relief for individuals aggrieved by unwarranted dissemination of criminal justice information. No court, however, has ever indicated that any standard such as reasonable suspicion should be used to curtail access to such information. In effect, the judiciary's refusal to impose such a restriction constitutes a recognition of the fact that the present balance between individual rights and the needs of law enforcement is drawn in the proper place. The "*Terry* test" requirement employed in Section 201(b)(1)(E) (and in Section 210(d)) would significantly alter the balance, even though no compelling reasons have been advanced for such a sweeping change.

Another problem arises from the fact that the Bill gives no indication of who is to determine whether the "*Terry* test" has been met. It is inevitable that there will arise at least some situations in which the officer accessing information and the agency disseminating it will disagree with the individual about whom the information relates as to whether the requisite *Terry* facts and inferences are present. In these borderline cases, the individual would be encouraged to bring suit. If he could show at trial that the officer and agency were incorrect in their assessment of whether the "*Terry* test" had been met, he could recover.

This would be the case regardless of whether the individual bringing suit had been charged or convicted as a result of the information disseminated. This possibility of the criminal successfully suing the officer or agency who acted in good faith (under Section 308 an officer or agency's own good faith is not a defense) is by no means far-fetched, since the "*Terry* test" is so subjective and since *Terry* itself has spawned an entire field of litigation. The effect of not allowing for a defense of good faith will be that criminal justice agencies will interpret the "*Terry* test" quite restrictively in order to guard against the possibility of being subjected to litigation. The test actually employed would, therefore, approach the Probable Cause Test. Such a restrictive test with regard to information to be used for the purpose of developing investigative leads prior to a determination of probable cause would be absurdly restrictive. For this reason, we strongly oppose a statutory requirement that the "*Terry* test" be employed.

To deny law enforcement agencies easy access to arrest and nonconviction record information would seriously hamper the agencies' abilities to focus investigations upon specific individuals. Although past arrests should not in themselves make an individual a suspect, it is unrealistic to assume that such information is not relevant during the formative stages of an investigation, at a time even before justification for a *Terry* stop could be shown. For instance, past arrest record information which indicated that an individual had used a standard modus operandi has often enabled investigators to focus upon that person and to subsequently uncover evidence tying that individual to the offense. S. 2008 would block access to such information.

The Justice Department Bill (S. 1428) employs a much more sensible approach by simply mandating that arrest record information accessed for the purpose of investigative leads could not without additional information provide the basis for a subsequent detention or arrest. This is the present state of the law and is a clearly rational restriction, since an individual's record alone could not

establish probable cause or even the requisite facts and inferences to justify a *Terry* stop. This standard, we believe, adequately strikes a balance between the rights of past criminals or suspects to be free from suspicion due to past crimes or alleged crimes and the crucial need of the public to allow law enforcement officers access to information useful in the investigation of offenses.

Section 202 is worded poorly. The resulting ambiguity could give rise to a restrictive interpretation which would seriously endanger the public. Section 201 provides severe restrictions on dissemination by criminal justice agencies of all forms of criminal justice information. Section 202 pinpoints certain specific exceptions to these dissemination restrictions for identification and wanted persons information. The exception relating to wanted persons information refers only to persons who are wanted for criminal offenses against whom judicial process has been issued. This language would not cover the situation where an individual who was validly arrested without a warrant escaped. A plain language reading of Sections 102(5), (6), 201 and 202 indicates that the police could not immediately broadcast a wanted persons bulletin for the escaped individual, since the broadcast would contain arrest information and no judicial process had yet been obtained. The absurdity of such a restriction is obvious; we assume it must be due to the ambiguity in the wording, rather than the intention of the drafters.

It is even conceivable that a more restrictive reading of Sections 201 and 202 could be given by an interpreting court or agency. Conceivably, Section 202 could be read as extending the restrictions of the Act so that no wanted persons information could be disseminated unless judicial process were outstanding. We do not believe that such a reading of Section 202 is called for, but we feel it important to point out the need to clarify the ambiguity.

Section 203(h) excepts from the general prohibitions of the Act certain disclosures by criminal justice agencies of factual information reasonably contemporaneous with the events to which the information relates. The scope of this provision should be clarified, since there could be conflicting interpretations of what constitutes the "event to which the information relates". It is not clear whether the event referred to in this section is the investigation or other action by a law enforcement agency, or the offense itself. Thus, it is uncertain whether a police department investigating a ring of organized criminals, but unable to link the ring to any recent crime, could disclose information about its investigation. We feel there are many occasions when the public and the press have a right to know intelligence or investigative information, even though the offense under investigation occurred at a past time. Disclosure of the findings of such investigations is often necessary in order to alert the public of the dangers posed by criminals and to inform the public of the steps police are taking to combat crime.

Section 206 requires all access to criminal justice information to be by name or other specific identifier unless either: (1) the information is accessed for criminal justice research, or (2) the disseminating agency has adopted procedures to insure that the information is used only for developing investigative leads for a specific offense and the requester has a need to know—right to know. Since access by category of offense or other general data element is permitted for research purposes, whether this provision of the Bill is unduly restrictive depends upon the interpretation of the word "research" as used in Section 203(d). The Bill does not define what is meant by "research." If the term were broadly defined, as we believe it should be, it could exempt from the requirement of access by specific identifier all statistical, analytical, and intelligence data not accessed for specific investigative or prosecutorial purposes. If, however, a narrow interpretation of "research" were employed, law enforcement agencies might not be able to develop needed evaluative tools, especially for intelligence purposes. In order to clear up any question of interpretation, the term "research" should be defined in Section 102.

Section 208 provides for the sealing and purging of criminal justice information. This section should be read together with Section 211(a), which requires the destruction of investigative information after the expiration of the statute of limitations for the offense concerning which it was collected or the sealing or purging of the criminal justice information related to the offense, whichever occurs later. Essentially, Section 208 requires the sealing of criminal justice information whenever an individual who has been convicted remains free from the jurisdiction or supervision of any criminal justice agency for seven years, unless the conviction was for an offense specifically exempted from sealing by statute. It also mandates the sealing of arrest record information if two years have elapsed since the arrest, detention or formal charge and no prosecution is pending and no conviction has been obtained. An exception to these sealing requirements is made if the

individual is a fugitive. This section further requires the *purging* of all criminal history record information whenever there has been a decision not to prosecute prior to the entrance of a formal charge.

The requirements for the sealing or purging of arrest record information in the event of non-prosecution are highly unrealistic. The realities of the criminal justice system are such that non-prosecution should not be equated with a finding of not guilty, since the decision not to prosecute may have been based on a tangential matter, such as the exclusion of essential evidence, or the decision of a key witness not to testify (as often happens in sex offense cases), or a public attitude opposed to full enforcement of certain laws. Although a check of old conviction or arrest records usually provides investigators with no substantive leads, old records do prove invaluable in the investigation of certain exceptional cases or classes of crimes. For instance, when an offense involves the same modus operandi as another offense, or occurs in an unusual location, a check of old records may often provide the needed clues for the development of an investigation.

As a specific example of how restrictive these provisions are, consider the following situation. Jane Doe reports that she was raped by John Smith. The police arrest John Smith and interrogate him. Since John Smith has no alibi and has given a very incoherent and contradictory explanation of his acts on the night of the rape, prosecutors believe that they have an air-tight case against him. Jane Doe, however, becomes terrified at the prospect of having the fact that she was raped publicized; as a result, she decides not to cooperate with the prosecution, and the prosecutor decides not to file a formal charge. This Bill would require the prompt purging of all information relating to John Smith's arrest for the alleged rape. Imagine the dilemma of the police if only a few months later another woman reports a rape at the same location as the attack against Jane Doe and gives a description of the assailant which corresponds to John Smith's appearance. Because of the provisions of Section 208(a) (4), the police would not have access to information relating to the previous arrest—information which would now be considered crucial in a criminal investigation.

Another key flaw of Section 208(a) stems from the failure of this section to consider the impact of cases where the accused is found not guilty because of insanity, or is not prosecuted because of his mental incompetence. In such cases, the defendant is usually civilly committed and must undergo psychiatric therapy and counseling. If a literal reading of Section 208(a) were employed, criminal justice information would have to be sealed, even while the individual was still civilly committed.

As another example of the difficulties created by the broad scope of Section 208(a), consider the problems faced by law enforcement agencies in their battle against organized crime. If the sealing and purging requirements of this section were put into effect, only 39 of the 282 records relating to the Gambino family would be unsealed. The same problem would exist as to almost all underworld leaders.

Section 208(b)(5) would require a criminal justice agency to obtain an access warrant before gaining access to sealed information. The test for obtaining access requires the requesting agency to show probable cause that it has "imperative need" for the information and that the information is not "reasonably available" from some other source. "Imperative need" is a vague standard, which could be interpreted quite restrictively and could bar law enforcement access to information needed during the early stages of an investigation. Likewise, Section 208(b)(5) gives no guidance for a court deciding whether the information is "reasonably available" from some other source. It should be specified that information is not "reasonably available" from another source when obtaining the information from the other source would involve inordinate expense or any significant delay or if the information obtained from the other source might be less accurate.

One other problem with this section centers on the jurisdictional requirements relating to the obtaining of access warrants. The procedures outlined in this section appear to require the requesting agency to obtain the warrant in the jurisdiction where the information system containing the information is located. This is an extreme inconvenience and a heavy burden; in most cases it will greatly increase the costs of obtaining even the simplest bits of sealed information. For example, this section would apparently require an agency in New Jersey which had arrested an individual who had previously resided in California to have a representative file suit in California in order to obtain the sealed records of the California criminal justice agencies. A further criticism of the access warrant requirement is that there is no provision allowing rapid access in cases where the delay required in getting the warrant may seriously impede the investigation.

Section 210(b) could be one of the most misguided provisions of the entire Bill, since it could severely restrict the ability of law enforcement agencies to engage in essential intelligence activities. Although we recognize the need to prevent intelligence operations from unnecessarily restricting the exercise of Constitutional rights, we must emphasize the dangers arising from the curtailment of legitimate intelligence activities. All recent major Commissions studying the problems of crime and disorder in this country have called for the creation of police intelligence units. The National Advisory Commission on Criminal Justice Standards and Goals in its Police Task Force Report stressed the need for intelligence by advising:

"Intelligence in the police sense is awareness. Awareness of community conditions, potential problems and criminal activity—past, present and proposed—is vital to the effective operation of law enforcement agencies, of continued security and safety."

A restrictive reading of Section 210(b) could ban all police intelligence activities except those directed at specific individuals who were actually suspected of criminal activity. The language of Sections 210(b) and 102(13) is not sufficiently specific. The standard stated in Section 210(b) restricting the maintenance of intelligence activity to only those situations where the criminal justice agency can show "grounds . . . connecting an individual with criminal activity" is too vague, since it could be interpreted to mean anything from a mere hunch to the existence of facts approaching probable cause. Here, as in a number of other areas, the presence of a civil damage remedy which does not provide for a defense of good faith may have serious consequences. Fear of being subjected to lawsuits might well lead law enforcement agencies and officers to be quite restrictive in their interpretations of Section 210(b), with the result that Section 210(b) as applied might be even more restrictive than envisioned by the drafters of this Bill.

Even if this standard were liberally interpreted, it would still be too restrictive, since individual bits of information collected for intelligence purposes often bear no direct connection with criminal activity. Frequently, it is only after an intelligence unit has amassed many seemingly insignificant bits of information and is able to fit these pieces together that a pattern of criminal activity can be uncovered. To require "grounds . . . connecting an individual with criminal activity" could prevent an agency from gathering these pieces of information before there was an actual investigation focusing on that individual. The effect of such a test would be to reduce intelligence data identifiable to specific individuals to little more than investigative information.

A restrictive interpretation could bar some of the most highly lauded intelligence operations against organized crime. Similarly, it might curtail law enforcement efforts to keep tabs on suspected assassins, terrorists or saboteurs. It could prevent police from gathering information necessary to prepare for mass gatherings, rallies and demonstrations. Since the restriction applies to all information relating to specific individuals, law enforcement agencies could not maintain intelligence records on protest group leaders unless the test outlined above was first met. Information relating to individuals attending protest rallies and demonstrations has often proven necessary to police trying to gauge the temper of expected demonstrators and to determine the extent of police presence which should be provided at the demonstration. Information on the leaders should be accessible regardless of whether there are any facts connecting them with criminal activities, since the purpose of intelligence activities relating to mass gatherings and demonstrations is usually not one of detecting criminals, but rather one of preventing disorder and violence.

Section 210(d) allows dissemination of intelligence information only to either: (1) a *Federal* agency authorized to receive such information for employment or security investigations, or (2) a criminal justice agency which can either meet the "*Terry* test" or needs it to confirm existing information. The criticisms of the use of the "*Terry* test" that were outlined in the discussion of Section 201(b)(1)(E) are even more weighty here, since intelligence information is by its nature preliminary and developmental. To allow exchange of information to state agencies only pursuant to the *Terry* test is to erase the effects of past steps toward cooperation among law enforcement agencies. For years, opponents of the organized crime syndicates have decried the lack of coordination between the many law enforcement agencies throughout the nation. In the past decade rudimentary steps toward consolidation of the attack on organized crime have been made through information pooling units, such as the nationwide Law Enforcement Intelligence Unit (L.E.I.U.) and state and regional information sharing networks

like the New York State Identification and Intelligence System (NYSIIS) and the New England Organized Crime Intelligence System (NEOCIS). The activities of such highly praised systems would be eliminated by this Bill.

Perhaps the most severe impact of Section 210(d) will be the prevention of the dissemination of intelligence information to intelligence units which have never requested the information. An agency possessing intelligence information often concludes that certain information may be needed by another agency, even though it might not possess enough facts and inferences to conclude that a crime is about to be committed in the jurisdiction to which the information would be disseminated. As a specific example, consider this common intelligence practice, which would be eliminated by Section 210(d). If an intelligence unit in jurisdiction A, which has an intelligence file on an organized crime figure who has operated in that jurisdiction, learns that the crime figure is planning to enter jurisdiction B, it will often notify jurisdiction B, even if it has no basis for ascertaining whether the crime figure is planning to commit a crime in jurisdiction B.

Jurisdiction A provides the information in order to alert jurisdiction B to the possibility of trouble, and the intelligence data disseminated enables the intelligence operations of jurisdiction B to be of maximum effectiveness. As another example, consider the situation where an intelligence unit has made a thorough investigation of a group of radicals who move from jurisdiction to jurisdiction. Section 210(d) would prevent the unit from disseminating this information or from accessing more information from other agencies unless it could meet the "*Terry* test," even though it might be possible to uncover a pattern of criminal activity and thus meet the "*Terry* test" only if the information of all the agencies was pooled. The overall effect of Section 210(d) would be to block information pooling and to destroy coordination of the efforts of the various intelligence units, so that organized criminals could seek refuge by moving from jurisdiction to jurisdiction.

We believe that the exchange of intelligence information within the law enforcement community should be permitted on a need to know—right to know basis, a standard which intelligence units now follow. Enforcement of this standard would prevent unnecessary dissemination of possibly scandalous or inaccurate information; but it would still enable law enforcement agencies to obtain intelligence data needed to develop coordinated analyses of organized crime and organized subversives.

There is an apparent conflict between the permissive provisions of Section 204(a) and the restrictive provisions of Section 210(d). Section 204(a) authorizes the dissemination of intelligence information to Federal, state and local government officials and legislative bodies considering certain appointments or nominations. Section 210(d) precludes all dissemination of intelligence information except as specifically authorized and refers only to the specific authorization granted to Federal agencies by Section 204. The contradiction between these two sections should be resolved, so that there is no possibility of an interpretation which would subject state and local officials and legislative bodies to greater restrictions than their Federal counterparts.

Another criticism of S. 2008 relating to intelligence operations arises from Section 210(f), which bans direct remote terminal access to all intelligence information. This restriction appears to be motivated by an unsubstantiated fear of modern technology and fails to recognize that properly administered automated systems can be more secure and accurate than manual systems. Fear of possible abuses should not result in a failure to recognize the value of computerization in the fight against organized crime and organized subversives. We feel that the value of an automated system like the LEAA-backed Interstate Organized Crime Index (IOCI) outweighs the possibility of abuse. IOCI presently contains only information which is already available to the public; it is gathered from public sources, such as public documents, congressional records and newspaper articles. So long as access to this type of computerized information is restricted to law enforcement officers on a need to know—right to know basis, there is little possibility of abuse or damage to an individual's reputation.

One interpretational problem exists concerning Section 211(a). This section would require the destruction of investigative information after the expiration of the statute of limitations for the offense concerning which it was collected or the sealing or purging of the criminal justice information related to that offense, whichever occurs later. This provision does not address the situation where investigative files are compiled concerning multiple offenses or multiple offenders. If an investigative file concerned a number of offenses, serious problems could arise in interpreting the phrase "for the offense concerning which it was collected."

Conceivably, this provision could require the destruction of the entire file upon the running of the shortest statute of limitations. On the other hand, it could be interpreted as not requiring destruction until the running of the longest statute of limitations. In order to avoid subsequent interpretational problems, this provision should be clarified.

Enforcement of S. 2008 would be through a joint state-Federal Commission on Criminal Justice Information to be established pursuant to Section 301. This section provides no assurance that the Commission will be properly representative of the interests primarily affected by the Bill. The key impact of this legislation would be upon state and local law enforcement agencies, but S. 2008 does not assure that Commission members drawn from the state and local criminal justice agencies will be truly representative. For instance, under S. 2008, the seven members from state and local agencies could all be from one component of the criminal justice system, or from one region of the nation. In order to assure that the Commission properly reflect the groups affected by the legislation, we would suggest a Commission composed of both Presidential appointees (subject to Senate approval) and members appointed by organizations representative of the various criminal justice agencies. As a specific example, we would propose a 17 member Commission. The Attorney General, two other Federal agency officials and two representatives of the public at large would be Presidential appointees. In addition, we would suggest that the President be allowed to appoint five members drawn from different size police departments: one member from a department with less than 100 employees, one from a department with between 100 and 500 employees, one from a department with between 500 and 1,500 employees, one from a department with more than 1,500 employees, and one from a state policy agency. These five representatives would be from five different states in various regions of the nation and would be subject to Senate confirmation. In addition to these ten Presidential appointees, we would suggest that seven organizational representatives be added to the Commission. These members would either be directly appointed by the organizations they represent or chosen by the President from lists of candidates submitted by the organizations. In order to assure diverse representation, we would propose that the range of the seven organizations be similar to the following: (1) Project SEARCH, (2) National District Attorneys' Association, (3) International Association of Chiefs of Police, (4) the Judicial Conference of the U.S., (5) the National Conference of Criminal Justice Planning Administrators, (6) the National Sheriffs Association, and (7) a professional corrections association. This type of distribution would assure that the Commission receives direct input by the state and local agencies most closely affected by this legislation.

If a truly representative Commission similar to the one we have suggested were established, the provision in Section 303 limiting the duration of the Commission to five years should be changed. In order to assure that state and local agencies continue to have a voice in the administration of the Act, the Commission should continue as long as the substantive provisions of the Act remain in effect.

One of our key criticisms of the Act arises from the extensive rulemaking powers granted to the Commission in Section 304(a)(1). When read together with the applicability provisions of Section 103, it becomes apparent that the Commission will be able, through the promulgation of rules and regulations, to dictate the procedures to be followed by state and local criminal justice agencies exchanging information intrastate. We have already emphasized our opposition to this intrusion upon the powers of the individual states. We wish to reiterate that the grant of extensive rulemaking power regarding intrastate information exchanges is unnecessary. This Bill appears to be motivated by a desire to establish some degree of uniformity. The only need for uniformity, we believe, exists with regard to interstate exchanges of information. Exchanges not involving the Federal government can be governed by formal written agreements; thus, there is no need to grant rulemaking powers to the Commission unless a state-Federal or local-Federal information exchange is concerned. Furthermore, there is no assurance that this legislation will eliminate present conflicts and complexities at the Federal level. Various Federal agencies now possess extensive rulemaking powers and would retain their powers after enactment of S. 2008. The possibility of conflict would still exist. Indeed, through the addition of one more agency, the possibility of conflict could actually be increased.

Long experience has shown that many of the key policy decisions of a commission, whose members meet only occasionally, are not made by the commissioners, but by their professional staff. Section 306 of S. 2008, by making the staff director a Presidential appointee, fails to recognize this reality. This Bill should include a

provision whereby the Commission can either choose the staff director or submit to the President a list of nominees. Such a provision would assure the Commission direct control over the staff director; otherwise, the state-Federal Commission might be little more than an advisory body to the full-time professional staff located in Washington.

Another serious defect in the Bill is Section 304(a)(5), which gives the Commission the power and the duty to publish an annual directory of criminal justice information systems. This directory would identify all systems and the nature, purpose and scope of each. Serious problems could arise as a result of making this directory available to criminals, who would be able to arrange their activities around the information printed in the directory. For example, organized criminals, as a result of knowledge gained from the directory, could plan to penetrate the information system and defeat all law enforcement efforts against them.

Section 308 is one of the key provisions of the Bill. It allows an aggrieved person to bring a civil action for violation of the Act or regulations promulgated pursuant to it. It is a sweeping damage remedy, which allows the successful plaintiff to recover, at a minimum, liquidated damages, attorneys' fees and costs. It also provides for exemplary and punitive damages, as well as injunctive relief. The only defense provided is the good faith reliance upon the assurance of another agency or employee. This defense is unquestionably too narrow. In contrast, the Justice Department Bill provided that one's own good faith interpretation of the Act or implementing rules, regulations and procedures would be a complete defense. By allowing only a narrow ground of defense, S. 2008 will punish officers for their good faith mistakes. The threat of punishment will, in turn, result in a chilling effect upon law enforcement efforts in any situation which might arguably violate the Act or rules and regulations. Thus, a realistic result of Section 308 will be to multiply the restrictive effects of all other provisions of the Act.

In conclusion, the IACP is opposed to S. 2008 in its present form because of its severe restrictions on the ability of law enforcement to fight crime and the encroachment by the Federal government on the traditional role of the states in the field of criminal justice. Although the individual's right to privacy is essential and is respected by law enforcement, consideration of the right to privacy must not unduly impede state and local law enforcement's fight against crime.

---

NATIONAL ASSOCIATION OF COUNTIES,
*Washington, D.C., July 21, 1975.*

Hon. JOHN V. TUNNEY,
*Chairman, Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, Washington, D.C.*

DEAR CHAIRMAN TUNNEY: I am enclosing copies of testimony from the National Association of Counties on S. 2008 for you and members Fong, Hruska, and Thurmond of the subcommittee. We understand our testimony will be read into the record of your hearings on this subject.

NACo's position can be summarized as follows: we believe standards must be set that guarantee the security and privacy of criminal-justice information, and militate against its misuse. But we cannot agree that exclusive dedication of data-processing hardware for criminal-justice information in any way provides this guarantee or helps prevent misuse. Rather, it imposes prohibitively costly requirements on state and local governments for new machines, accessories, and programming. Many local governments would be forced by S. 2008 to turn their criminal-justice information over to a state-wide system, decreasing their ability to plan for reduction of crime and administration of justice within their own borders.

We very much appreciate the forum your subcommittee has created to hear all sides of this issue.

Sincerely,

RALPH L. TABOR,
*Director, Office of Federal Affairs.*

---

PREPARED STATEMENT OF THE NATIONAL ASSOCIATION OF COUNTIES

NACo firmly opposes inclusion of any language in S. 2008 requiring that criminal-justice information systems employ hardware exclusively dedicated to criminal-justice purposes, or that management control of this hardware be

exercised only by a criminal-justice agency. Earlier versions of the bill include these requirements, as do U.S. Department of Justice guidelines [40 FR 22114–9 (1975)]. We are convinced these requirements would be prohibitively expensive to implement and do little to increase individual privacy.

Shared-use computers are common in the business world. Often the same hardware processes and stores sensitive information of numerous corporations. This prudent and economical practice is also followed by most counties administering local, automated information systems. They employ a single large machine for numerous functions.

Experience in both the public and private sectors overwhelmingly indicates that individual files can be protected from unauthorized electronic linkage to other files, and protected from direct access by unauthorized users.

The greatest danger for abuse is not that files will be linked to create an electronic "dossier," or that an unauthorized user will be able to activate a terminal to access data. The greatest danger for abuse is the unauthorized use of data by authorized users. This must be dealt with by proper software control and rigorous enforcement procedures. In large measure, it is a personnel control problem, unaffected by whether the computer is exclusively dedicated to any functional area of government responsibility. The need to vest management control of hardware in a criminal-justice agency, while dealing indirectly with the problem of personnel control, is simply unsupported by experience. The history of administration of sensitive records by local, state, and federal criminal-justice agencies hardly supports the claim that they, alone, are capable of protecting individual privacy. It may well be that an outside agency investigating violators of security and requiring punishment of violators can reduce the incidence of leakage of personnel information. There is certainly no evidence to indicate that external agencies are unable to carry out this function.

In addition to missing the basic point, these requirements will be very expensive to implement. The need to acquire substantial amounts of new hardware, accessories, and software would prohibit all but the very largest local governments from automating criminal-justice information.

Local governments, unable to meet the costs of exclusively dedicated equipment, would be forced to rely on large state-wide systems. The advent of these systems would cause many difficulties, and threaten the very privacy that exclusive dedication is alleged to protect.

Local criminal-justice information systems often contain data that are not accessible through state or national networks. While we believe that it is important to regulate the kinds of data stored in local systems, it is also important to note that much data does not flow into state and federal systems. The demise of local systems would result in the transfer of all of this data to the state. The result is a large system that may well make more data available to more people.

Local systems also provide the flexibility that permits the generation of aggregate data necessary for planning and management. Case flows, response-time by police, court dockets, are only a few of these activities. A state system simply could not provide this information to its many municipalities in a timely fashion.

Finally, the Department of Justice and others have indicated they feel that exclusive dedication will not impose a heavy financial burden on local government. They base this assumption on the expected arrival of inexpensive "mini-computers." We do not believe this expectation is realistic. First, it ignores the heavy investment in current equipment. Second, mini-computers do not have the flexibility to carry out the many on-line inquiry and management functions required of a local information system.

SUMMARY

The National Association of Counties believes requirements for exclusive dedication and management control by criminal-justice agencies of criminal-justice information should not be included in S. 2008. These are operational decisions state and local governments should properly make. The federal government should set standards, as it does in S. 2008. But standards should not be set that impose costly, ineffective requirements on the state and local governments that implement the standards.

SEARCH GROUP, INC.,
*Sacramento, Calif., May 27, 1975.*

Senator JOHN TUNNEY,
*Dirksen Building,*
*Washington, D.C.*

DEAR SENATOR TUNNEY: In response to a request from the Law Enforcement Assistance Administration, Search Group, Inc. has had the opportunity to

review and comment on House of Representatives' Bill 61 (corresponding to Senate Bill 1428). The Search Group, Inc. membership, representing the views and interests of the state and local criminal justice community, identified specific areas of the Bill it considered to be of major concern. This review, involving a number of SGI committees, was conducted the week of May 12, 1975.

Recognizing your concern and interest in this legislation, Search Group, Inc. is providing you with a copy of the report it has sent to LEAA for your information and ready reference. The attached report recommends changes to the Bill which, if complied with, would bring H.R. 61 into consonance with the position on security and privacy developed by SGI over the last several years.

As a forum for developing consensus among state and local criminal justice agencies, Search Group, Inc. recognizes its responsibility to address issues of this magnitude. We trust that these comments will be of assistance to you in your deliberations, and in the future we offer continued assistance to the Congress on such matters.

Sincerely,

GARY D. MCALVEY, *Chairman.*

Attachment.

SEARCH GROUP, INC.

REPORT ON H.R. 61 [CORRESPONDING TO S. 1428]

Search Group, Inc. has reviewed H.R. 61 and has compared its provisions with previous positions on security and privacy adopted by Search. Many of the security and privacy principles supported by Search are embodied in H.R. 61. However, some principles recommended by Search are not included in the bill. The major deficiencies in the bill are set forth below. If the bill were amended to correct these deficiencies, SEARCH Group, Inc. could support it.

Recommendations 2, 4, 5, 9, 10, 12, 13 and 18 are essential to the development of security and privacy legislation acceptable to Search Group, Inc.

Recommendations 1, 3, 6, 7, 8, 11, 14, 15, 16 and 17 are less critical, but are also necessary to make H.R. 61 consistent with previous Search positions.

The recommended changes are:

1. That section 102(6), which defines "criminal justice agency," be clarified to ensure that the term includes any agency that is empowered by statute or executive order to act as a repository of criminal justice information or to provide services involving the collection, maintenance or dissemination of such information.

2. That section 201(c), which sets out restrictions on the use by criminal justice agencies of arrest records, be amended to apply to both arrest records and to records that indicate that the individual was acquitted or that charges were dropped or dismissed or otherwise disposed of in the individual's favor, and to include the *additional* restriction that such records may be used only for the following purposes:

(*a*) employment screening by criminal justice agencies;

(*b*) supervision of the arrested individual and adjudication of the charges growing out of the arrest;

(*c*) investigation of an individual who has been arrested or detained;

(*d*) investigation of an individual who has not been arrested or detained, *provided* that there is evidence (sufficient to meet the constitutional standards set forth in *Terry v. Ohio*) indicating that the individual is or may be involved in criminal activity and that the arrest or nonconviction information may be relevant to the investigation.

(*e*) the alerting of law enforcement officers that the individual may be dangerous; and

(*f*) similar essential purposes to which the information is relevant, as specifically defined in criminal justice agency regulations or operating procedures.

3. That section 203(a), relating to formal written agreements governing inter-agency automated exchanges of information, be deleted on the grounds that it would be difficult to implement and would not serve any purpose not otherwise adequately provided for in the bill.

4. That section 203(b), relating to access to information stored in automated systems, be amended to include the following additional provisions:

(*a*) access to arrest records and criminal offender records maintained in automated systems should be available only if the inquiry is based upon identification of the subject individual by name or other personal identifiers. Prior to the arrest of an individual, inquiries should be based upon the most reliable identification information available to the requesting agency, even though a positive

identification of the individual may not be possible. After the arrest or detention of the individual, inquiries should be based upon a positive identification of him by means of fingerprints or other reliable identification information.

(*b*) notwithstanding subsection (a), automated information systems should be permitted to respond to requests for arrest records and conviction records based upon categories of offense or other "class access" data elements, provided that operating procedures are in effect to insure that the information is used only for the purpose of developing investigative leads for particular criminal offenses and that the information shall be available only to criminal justice officers and employees with authority and a particular need to receive it.

(*c*) automated access to nonconviction records (where the individual was acquitted, charges were formally dropped or dismissed or the proceedings were otherwise concluded in the defendant's favor) based upon class data elements rather than individual identification information should be permitted only upon the issuance by a judge or magistrate of a class access warrant based upon a showing of probable cause that—

(1) such access is imperative for the investigation of a particular criminal offense; and

(2) the information sought is not obtainable from other sources or through any other means.

5. That subsections (a), (b) and (c) of section 204, relating to noncriminal justice uses of criminal justice information, be amended to provide that, except for the uses expressly authorized in subsections (d), (e) and (f) or elsewhere in the bill, no use of criminal justice information for a noncriminal justice purpose shall be permitted unless—

(*a*) such dissemination and use are expressly authorized by federal or state law;

(*b*) the information available is limited to conviction records and arrest records where the arrest is not over a year old and the charges are still actively pending;

(*c*) release of the information is not prohibited by law in the state where the arrest or conviction occurred; and

(*d*) the individual subject has been notified by the requesting agency or person that the request has been made and that he has a right to review the information and to initiate proceedings for challenge or correction of any inaccurate or incomplete information.

6. That section 205(b), which authorizes the dissemination of criminal justice information, including intelligence and investigative information, for use in federal employment investigations and security clearance investigations, be amended to provide that criminal justice investigations and intelligence information may be disseminated and used for security clearance investigations by federal agencies, but not for employment investigations.

7. That paragraph (3) of section 207(a), requiring that subsequently received information relating to arrest records or criminal records be promptly disseminated to earlier recipients of such records, be amended to require the dissemination of such additional information to the persons or agencies from which the original record was received and to all persons or agencies that have received the record during the period that audit records of disseminations are required to be kept.

8. That paragraphs (4) and (5) of section 207(a), relating to the keeping of records of the sources and recipients of arrest records and criminal offender records, be amended to require the retention for at least three years of records of—

(*a*) the source of arrest record information and criminal offender record information; and

(*b*) the identity of other agencies or persons who request or receive arrest record information, criminal offender record information, criminal intelligence information or criminal investigative information, together with the date of each request, the authority of the requestor, the purpose of the request, the disposition of the request and the nature of any information provided.

9. That subsections (c) and (d) of section 207, relating to sealing and purging, be deleted and replaced by provisions embodying the following principles:

(*a*) Each criminal justice information system should adopt procedures to insure that arrest records and criminal offender records are sealed or purged when required by federal or state statute, regulation or court order. In addition, such procedures should provide, as a minimum, for the sealing of—

(1) arrest records not followed by formal charges or where prosecution is declined or dismissed;

(2) arrest records not followed by a conviction within two years of the arrest or detention, if prosecution is not actively pending at the end of that period and if the individual is not a fugitive;

(3) felony conviction records if the individual has been free of criminal involvement for a period of seven years following final release from confinement or supervision, unless the conviction record has been specifically exempted from sealing under federal or state law; and

(4) misdemeanor conviction records if the individual has been free of criminal involvement for a period of five years following final release from confinement or supervision.

(*b*) Sealing should be accomplished by some procedure that, as a minimum, removes the sealed information from routinely available status to a status requiring special procedures for access.

(*c*) Sealing and purging should be accomplished in fully automated systems at intervals as frequent as feasible, and, in systems in which the sealing and purging process is not automated, upon request for access to the information or upon receipt of a court order or other formal notice that immediate sealing or purging is required.

(*d*) Sealed records should be permitted to be made available—

(1) for research, evaluative and statistical purposes;

(2) for review by the individual for purposes of challenge or correction;

(3) for audit purposes;

(4) if the individual is subsequently arrested for an offense which is subject to imposition of a higher sentence under a federal or state statute providing for additional penalties for repeat or habitual offenders;

(5) if subsequent criminal charges are filed against the individual; and

(6) upon court order.

(*e*) The legislation should permit the maintenance of indexes of sealed records to facilitate access to the records under the above paragraph. Access to such an index should be limited to authorized officials and employees of criminal justice agencies who need access for one of the purposes enumerated above or for investigation purposes if there is evidence (sufficient to meet the constitutional standard set forth in *Terry* v. *Ohio*) that a particular individual is or may be involved in a criminal activity and a sealed record may be relevant to the investigation.

10. That section 209(a), relating to intelligence and investigative files, be amended to provide that—

(*a*) criminal intelligence information concerning an individual may be collected and maintained only if grounds exist connecting the individual with known or suspected criminal activity to which the information is relevant, and

(*b*) criminal intelligence files should be reviewed at regular intervals—and, at a minimum, upon request for particular information—and destroyed if grounds for retaining the files no longer exist.

11. That section 209(b)(2), relating to inter-agency exchange of intelligence and investigative information, be amended to provide that criminal intelligence, information may be disseminated outside of the collecting agency only to another criminal justice agency and only for the following purposes—

(*a*) employment screening by criminal justice agencies;

(*b*) confirmation of information in the files of another criminal justice agency; and

(*c*) for purposes of investigation of the individual subject if constitutionally valid grounds for the investigation exist and the information is relevant to the investigation.

12. That section 209(c), which prohibits direct terminal inter-agency access to automated intelligence and investigative files unless authorized by federal or state law or executive order, be amended to permit direct terminal access to "public record" information maintained in such files and to identification information sufficient to provide an index of individuals whose files are included in automated systems and to refer any requesting agency to the agencies maintaining the files.

13. That sections 301–305, which establish a Commission on Criminal Justice Information, be amended to provide that the Commission—

(*a*) be composed of members from federal departments and agencies, state and local criminal justice agencies representing all segments of the criminal justice system, and the private sector with state and local criminal justice agency representatives comprising a majority of the membership;

(*b*) be empowered to issue rules, regulations, and orders governing all criminal justice information systems—including any national interstate systems such as NCIC–CCH—except systems that contain only records relating to federal offenses and that do not exchange information with state or local criminal justice agencies.

(*c*) be empowered to conduct reviews and audits of all systems subject to the legislation to insure compliance with the legislation and the Commission's regula-

tions, to enforce appropriate sanctions against agencies and individuals found in violation and to bring appropriate administrative and judicial actions; and

(*d*) be required to comply with the Administrative Procedures Act in issuing regulations and to consult specifically with groups such as Search Group, Inc. that represent state and local criminal justice agencies and information systems prior to issuing regulations, orders or interpretations that affect the collection, dissemination or use of criminal justice information maintained by state or local criminal justice agencies.

14. That section 307, relating to judicial remedies, be amended to include a criminal penalty applicable to willful and knowing violations of any of the provisions of the legislation relating to the maintenance, dissemination or use of criminal justice information.

15. That section 308, which provides that state or local agencies operating or participating in systems subject to the legislation shall be deemed to have consented to suit under the legislation, be amended by adding a similar consent-to-suit provision applicable to the Federal Government.

16. That a provision be added to the bill requiring criminal justice agencies to publish annual public notice of the existence and nature of each criminal justice information system it maintains—except manual systems that contain less than 10,000 individual records—reasonably designed to acquaint the public with the nature of the system, including the categories of data and subjects in the system, uses permitted of the data and the operational policies and procedures governing the system.

17. That a provision be added to the bill providing for the establishment in the states of boards or agencies with statewide authority to regulate criminal justice information systems and oversee compliance with federal and state legislation.

18. That a provision be added to the bill authorizing the establishment of a national interstate criminal record information system to facilitate the exchange among state and federal criminal justice agencies of arrest records, criminal offender records, correctional and release information, wanted persons information and identification information. The provision should—

(*a*) specify the extent to which federal criminal justice agencies may participate in such a system, including whether a federal agency may provide central information maintenance facilities or telecommunications facilities for the interstate transmission of information;

(*b*) limit the maintenance of criminal records at the federal level in such a system to the following—

(1) federal and foreign records;

(2) records of individuals with offenses in two or more states; and

(3) records of felony offenses submitted by states that otherwise would not be able to participate fully in the national system because of the lack of facilities and procedures, but only for a period of five years after the effective date of the legislation; and

(*c*) provide that, as to all other records, the national system shall be limited to the maintenance of personal identification information sufficient to provide an index of individuals with records maintained in the system and an indication of the identity and location of criminal justice agencies maintaining such records.

---

## Prepared Statement of the United States League of Savings Associations [1]

The United States League of Savings Associations appreciates this opportunity to file a statement on the "Criminal Justice Information Control and Protection of Privacy Acts," S. 1428 and S. 2008.

---

[1] The United States League of Savings Associations (formerly the United States Savings and Loan League) has a membership of 4,600 savings and loan associations, representing over 98% of the savings and loan business. League membership includes all types of associations—Federal and state-chartered, insured and uninsured, stock and mutual. The principal officers are: Lloyd S. Bowles, President, Dallas, Texas; Robert Hazen, Vice President, Portland, Oregon; Tom B. Scott Jr., Legislative Chairman, Jackson, Mississippi; Norman Strunk, Executive Vice President, Chicago, Illinois; Arthur Edgeworth, Director-Washington Operations; and Glen Troop, Legislative Director. League headquarters are at 111 East Wacker Drive, Chicago, Illinois 60601; and the Washington Office is located at 1709 New York Avenue, N.W., Washington, D.C. 20006; Telephone: 785-9150.

We favor legislation which would authorize our members (and other financial institutions) to have access to FBI criminal record information. We believe that the present section of the Department of Justice Appropriations Act of 1973 (PL 92–544), which authorizes savings and loan associations access to FBI criminal record information, should remain in effect. We feel that the language of S. 1428 provides our members with the necessary authority to continue to receive this information. We urge that any legislation reported by this Subcommittee specifically authorize our members continued access to criminal record information.

We support legislation which would protect the individual's right to privacy; provide the individual with access to his own records for correction and verification; establish standards for dissemination of criminal justice information; and insure the accuracy and thoroughness of criminal justice records. At the same time, we urge the Subcommittee to recognize the legitimate needs for access to criminal justice information by criminal justice agencies, as well as certain non-criminal justice agencies including savings and loan associations. Our comments are directed at those sections of the bills which affect the access by savings and loan associations to the criminal record information system provided by the FBI.

Savings and loan associations[2] are authorized by the Department of Justice Appropriations Act of 1973 to receive FBI identification records on employees or applicants for employment "to promote or maintain the security of those institutions". This service has been an invaluable aid to savings and loan associations because it usually brings to their attention the prior criminal record of any potential employee who would handle or have access to the monies of not ouly private citizens and business firms, but also local, state and Federal government agencies. The embezzler, thief or individual who has been convicted of a crime involving breach of trust or dishonesty, or has a history of such conduct, generally has no place as an employee of a financial institution. Our experience has demonstrated that access by our members to FBI criminal record information is essential if they are to meet their obligation to depositors, borrowers and the general public who see the integrity of financial institutions as a reflection of the character of the institution's employees, officers and directors.

This obligation to know the background of potential employees is not only one of common sense and good management practice, but is incident to the proper conduct of the institution as prescribed by Federal statute and regulation. 12 USC 1730(h) and 12 USC 1464(d)(5)(a) authorize the suspension of any officer or director of a Federally-insured savings and loan association if the individual is charged with a felony involving dishonesty or breach of trust. A conviction for such an offense could then result, and in almost all cases does result, in automatic removal from office and a specific prohibition from further involvement in the business affairs of the institution. Also, except with the prior written consent of the Federal Home Loan Bank Board or the FSLIC, the primary regulatory agency and insuring agency for Federal and many state savings and loan associations, no individual who has been convicted of a criminal offense involving dishonesty or breach of trust can serve as an officer, director or employee of a savings and loan association. Willful violation of this requirement subjects the savings and loan association to a penalty of up to $100 for each day that the prohibition is violated. (12 USC 1464(d)(12)(B); 12 USC 1730(p)(2)).

The significance of the receipt of FBI criminal record information by savings and loan associations is also demonstrated by an official memorandum of the Federal Home Loan Bank Board's Office of Examinations and Supervision which requires that every Federally-insured institution be informed of the availability

---

[2] The Department of Justice Appropriations Act gives special recognition to Federally-chartered and Federally-insured savings and loan associations. All Federally-chartered associations are regulated by the Federal Home Loan Bank Board and insured by the Federal Savings and Loan Insurance Corporation. Most state-chartered associations are insured by FSLIC. These associations account for approximately 89% of our members. For purposes of this statement, the term "savings and loan association" refers to Federally-chartered and Federally-insured savings and loan associations.

We also believe that all savings and loan associations should have access to FBI criminal record information. This would include not only Federally-chartered and Federally-insured associations, but also members of the Federal Home Loan Bank System; such as, the cooperative banks in Massachusetts and various savings and loan associations in Maryland and Ohio, the accounts of which are insured by state-chartered insurance corporations.

of this service and recommends that all savings and loan associations provide the FBI with fingerprint cards of their officers, directors and employees.

(Memorandum 44–2, December 22, 1971) Examiners of the Office of Examinations and Supervision also frequently urge the adoption of this procedure during the course of their examination of savings and loan associations.

S. 2008 provides for the dissemination of conviction and arrest record information to non-criminal justice agencies in certain specified instances as well as under express authorization by Federal or state statute. (Section 203(a)(b)). S. 2008 also specifically repeals the existing statutory authority for access by savings and loan associations to this information (Section 314(a)). Specific statutory language would be required to continue this access.

S. 1428 provides for the dissemination of criminal record information to non-criminal justice agencies as provided by the bill or as authorized by Federal or state statute or Executive order (Section 204(a)). The bill further authorizes a criminal justice agency to provide "criminal record information to federally-chartered or insured financial institutions for purposes of employment review" (Section 205(c)). S. 1428 also repeals the existing statutory authority for access by savings and loan associations to this information (Section 311).

It should also be noted that an existing FBI regulation limits the dissemination of criminal record information in instances in which the arrest is more than one year old to information including a disposition of the arrest (28 CFR 50.12).

The U.S. League believes that both of these bills would have the most beneficial impact on the savings and loan association and its prospective and present employees, officers and directors by their provisions which insure that criminal record information received by the association is accurate and complete. Records which reflect a case of mistaken identity are inherently damaging to the individual. Further, they are of no value to the savings and loan association. A record which does not reflect a disposition of the arrest, where such is available, does a disservice to both the individual and the savings and loan association. Our members who use FBI record information, do so with discretion and with an attitude which recognizes that this information is only one of several factors to be considered in evaluating potential employees.

The result is not a blanket denial of employment because of the mere fact of an arrest, a youthful indiscretion or an unwarranted arrest. Instead, each item of record data is only one element to be balanced with the other aspects of an individual's background upon which the savings and loan association selects its employees. At the same time, we feel that the arrest of an individual for embezzlement, even though standing alone should not be a bar to employment, is a fact which deserves further explanation by the prospective employee who will have access to funds of the association.

We would also like to briefly comment on the provision of S. 2008 which provides for the sealing or purging of criminal justice information. We understand the need to give an individual a fresh start so that his record does not unnecessarily or unfairly follow him throughout his life. At the same time, we feel that more study should be given to the impact on the individual and the institution of the purging or sealing of records with an eye to establishing an initial period for purging or sealing after fifteen years rather than the proposed seven-year period. Savings and loan associations still have the same responsibility under 12 USC 1464(d)(12)(B) and 12 USC 1730(p)(2) whether a conviction involving dishonesty or breach of trust is five or fifty years old, and any legislation in this area should give recognition to this potential conflict.

In conclusion, we believe that savings and loan associations should continue to have access to FBI criminal record information, and therefore, favor the language of S. 1428.

We urge the Subcommittee to recognize the legislative and regulatory requirements placed on savings and loan associations as cited above; and in any reported bill, specifically authorize access by Federally-insured and Federally-chartered savings and loan associations, at the very least, to criminal record information which would satisfy these requirements. We will be happy to assist the Subcommittee and respond to any further inquiries on what we believe represents an issue of vital concern to the individual, as well as the savings and loan association.

## ARTICLES FOR THE RECORD

[From the Federal Register, May 20, 1975]

DEPARTMENT OF JUSTICE—CRIMINAL JUSTICE INFORMATION SYSTEMS

TITLE 28—JUDICIAL ADMINISTRATION

CHAPTER I—DEPARTMENT OF JUSTICE

[Order No. 601-75]

PART 20—CRIMINAL JUSTICE INFORMATION SYSTEMS

This order establishes regulations governing the dissemination of criminal record and criminal history information and includes a commentary on selective sections as an appendix. Its purpose is to afford greater protection of the privacy of individuals who may be included in the records of the Federal Bureau of Investigation, criminal justice agencies receiving funds directly or indirectly from the Law Enforcement Assistance Administration, and interstate, state or local criminal justice agencies exchanging records with the FBI or these federally-funded systems. At the same time, these regulations preserve legitimate law enforcement need for access to such records.

Pursuant to the authority vested in the Attorney General by 28 U.S.C. 509, 510, 534, and Pub. L. 92-544, 86 Stat. 1115, and 5 U.S.C. 301 and the authority vested in the Law Enforcement Assistance Administration by sections 501 and 524 of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Pub. L. 93-83, 87 Stat. 197 (42 U.S.C. § 3701 et seq. (Aug. 6, 1973)), this addition to Chapter I of Title 28 of the Code of Federal Regulations is issued as Part 20 by the Department of Justice to become effective June 19, 1975.

This addition is based on a notice of proposed rule making published in the FEDERAL REGISTER on February 14, 1974 (39 FR 5636). Hearings on the proposed regulations were held in Washington, D.C. in March and April and in San Francisco, California in May 1974. Approximately one hundred agencies, organizations and individuals submitted their suggestions and comments, either orally or in writing. Numerous changes have been made in the regulations as a result of the comments received.

Sec.

Subpart A—General Provisions



Subpart B—State and Local Criminal History Record Information Systems



Subpart C—Federal System and Interstate Exchange of Criminal History Record Information



AUTHORITY: Pub. L. 93-83, 87 Stat. 197, (42 U.S.C. 3701, et seq.; 28 U.S.C. 534), Pub. L. 92-544, 86 Stat. 1115.

SUBPART A—GENERAL PROVISIONS

*§ 20.1 Purpose*

It is the purpose of these regulations to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the completeness; integrity, accuracy and security of such information and to protect individual privacy.

*§ 20.2 Authority*

These regulations are issued pursuant to sections 501 and 524(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Pub. L. 93–83, 87 Stat. 197, 42 U.S.C. 3701, et seq. (Act), 28 U.S.C. 534, and Pub. L. 92–544, 86 Stat. 1115.

*§ 20.3 Definitions*

As used in these regulations:

(a) "Criminal history record information system" means a system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation or dissemination of criminal history record information.

(b) "Criminal history record information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system.

(c) "Criminal justice agency" means: (1) courts; (2) a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

(d) The "administration of criminal justice" means performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

(e) "Disposition" means information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the nature of the termination in the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Dispositions shall include, but not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed—civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial—defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

(f) "Statute" means an Act of Congress or State legislature of a provision of the Constitution of the United States or of a State.

(g) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(h) An "executive order" means an order of the President of the United States or the Chief Executive of a State which has the force of law and which is published in a manner permitting regular public access thereto.

(j) "Act" means the Omnibus Crime Control and Safe Streets Act, 42 U.S.C. 3701 et seq. as amended.

(j) "Department of Justice criminal history record information system" means the Identification Division and the Computerized Criminal History File systems operated by the Federal Bureau of Investigation.

Subpart B—State and Local Criminal History Record Information Systems

§ *20.20 Applicability*

(a) The regulations in this subpart apply to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July 1, 1973, pursuant to Title I of the Act.

(b) The regulations in this subpart shall not apply to criminal history record information contained in: (1) posters, announcements, or lists for identifying or apprehending fugitives or wanted persons; (2) original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis; (3) court records of public judicial proceedings compiled chronologically; (4) published court opinions or public judicial proceedings; (5) records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators' licenses; (6) announcements of executive clemency.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates. Nor is a criminal justice agency prohibited from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by paragraph (b) of this section.

§ *20.21 Preparation and submission of a Criminal History Record Information Plan*

A plan shall be submitted to LEAA by each State within 180 days of the promulgation of these regulations. The plan shall set forth operational procedures to—

(a) *Completeness and accuracy.* Insure that criminal history record information is complete and accurate.

(1) Complete records should be maintained at a central State repository. To be complete, a record maintained at a central State repository which contains information that an individual has been arrested, and which is available for dissemination, must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred. The above shall apply to all arrests occurring subsequent to the effective date of these regulations. Procedures shall be established for criminal justice agencies to query the central repository prior to dissemination of any criminal history record information to assure that the most up-to-date disposition data is being used. Inquiries of a central State repository shall be made prior to any dissemination except in those cases where time is of the essence and the repository is technically incapable of responding within the necessary time period. (2) To be accurate means that no record containing criminal history record information shall contain erroneous information. To accomplish this end, criminal justice agencies shall institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information and upon finding inaccurate information of a material nature, shall notify all criminal justice agencies known to have received such information.

(b) *Limitations on dissemination.* Insure that dissemination of criminal history record information has been limited, whether directly or through any intermediary only to:

(1) Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment;

(2) Such other individuals and agencies which require criminal history record information to implement a statute or executive order that expressly refers to criminal conduct and contains requirements and/or exclusions expressly based upon such conduct;

(3) Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement. The agreement shall specifically authorize

access to data, limit the use of data to purposes for which given, insure the security and confidentiality of the data consistent with these regulations, and provide sanctions for violation thereof;

(4) Individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. The agreement shall specifically authorize access to data, limit the use of data to research, evaluative, or statistical purposes, insure the confidentiality and security of the data consistent with these regulations and with section 524(a) of the Act and any regulations implementing section 524(a), and provide sanctions for the violation thereof;

(5) Agencies of State or federal government which are authorized by statute or executive order to conduct investigations determining employment suitability or eligibility for security clearances allowing access to classified information; and

(6) Individuals and agencies where authorized by court order or court rule.

(c) *General policies on use and dissemination.* Insure adherence to the following restrictions:

(1) Criminal history record information concerning the arrest of an individual may not be disseminated to a non-criminal justice agency or individual (except under § 20.21(b) (3), (4), (5), (6)) if an interval of one year has elapsed from the date of the arrest and no disposition of the charge has been recorded and no active prosecution of the charge is pending;

(2) Use of criminal history record information disseminated to non-criminal justice agencies under these regulations shall be limited to the purposes for which it was given and may not be disseminated further.

(3) No agency or individual shall confirm the existence or non-existence of criminal history record information for employment or licensing checks except as provided in paragraphs (b)(1), (b)(2), and (b)(5) of this section.

(4) This paragraph sets outer limits of dissemination. It does not, however, mandate dissemination of criminal history record information to any agency or individual.

(d) *Juvenile records.* Insure that dissemination of records concerning proceedings relating to the adjudication of a juvenile as delinquent or in need or supervision (or the equivalent) to non-criminal justice agencies is prohibited, unless a statute or Federal executive order specifically authorizes dissemination of juvenile records, except to the same extent as criminal history records may be disseminated as provided in § 20.21(b) (3), (4), and (6).

(e) *Audit.* Insure that annual audits of a representative sample of State and local criminal justice agencies chosen on a random basis shall be conducted by the State to verify adherence to these regulations and that appropriate records shall be retained to facilitate such audits. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated.

(f) *Security.* Insure confidentiality and security of criminal history record information by providing that wherever criminal history record information is collected, stored, or disseminated, a criminal justice agency shall—

(1) Institute where computerized data processing is employed effective and technologically advanced software and hardware designs to prevent unauthorized access to such information;

(2) Assure that where computerized data processing is employed, the hardware, including processor, communications control, and storage device, to be utilized for the handling of criminal history record information is dedicated to purposes related to the administration of criminal justice;

(3) Have authority to set and enforce policy concerning computer operations;

(4) Have power to veto for legitimate security purposes which personnel can be permitted to work in a defined area where such information is stored, collected, or disseminated;

(5) Select and supervise all personnel authorized to have direct access to such information;

(6) Assure that an individual or agency authorized direct access is administratively held responsible for (i) the physical security of criminal history record information under its control or in its custody and (ii) the protection of such information from unauthorized accesses, disclosure, or dissemination;

(7) Institute procedures to reasonably protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or man-made disasters;

(8) Provide that each employee working with or having access to criminal history record information should be made familiar with the substance and intent of these regulations; and

(9) Provide that direct access to criminal history records information shall be available only to authorized officers or employees of a criminal justice agency.

(g) *Access and review.* Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that—

(1) Any individual shall, upon satisfactory verification of his identity be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;

(2) Administrative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided:

(3) The State shall establish and implement procedures for administrative appeal where a criminal justice agency refuses to correct challenged information to the satisfaction of the individual to whom the information relates;

(4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;

(5) The correcting agency shall notify all criminal justice recipients of corrected information; and

(6) The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigatory, or other related files and shall not be construed to include any other information than that defined by § 20.3(b).

*§ 20.22 Certification of Compliance.*

(a) Each State to which these regulations are applicable shall with the submission of each plan provide a certification that to the maximum extent feasible action has been taken to comply with the procedures set forth in the plan. Maximum extent feasible, in this subsection, means actions which can be taken to comply with the procedures set forth in the plan that do not require additional legislative authority or involve unreasonable cost or do not exceed existing technical ability.

(b) The certification shall include—

(1) An outline of the action which has been instituted. At a minimum, the requirements of access and review under 20.21(g) must be completely operational;

(2) A description of any legislation or executive order, or attempts to obtain such authority that has been instituted to comply with these regulations;

(3) A description of the steps taken to overcome any fiscal, technical, and administrative barriers to the development of complete and accurate criminal history record information;

(4) A description of existing system capability and steps being taken to upgrade such capability to meet the requirements of these regulations; and

(5) A listing setting forth all non-criminal justice dissemination authorized by legislation existing as of the date of the certification showing the specific categories of non-criminal justice individuals or agencies, the specific purposes or uses for which information may be disseminated, and the statutory or executive order citations.

*§ 20.23 Documentation: Approval by LEAA.*

Within 90 days of the receipt of the plan, LEAA shall approve or disapprove the adequacy of the provisions of the plan and certification. Evaluation of the plan by LEAA will be based upon whether the procedures set forth will accomplish the required objectives. The evaluation of the certification(s) will be based upon whether a good faith effort has been shown to initiate and/or further compliance with the plan and regulations. All procedures in the approved plan must be fully operational and implemented by December 31, 1977, except that a State, upon written application and good cause, may be allowed an additional period of time to implement § 20.21(f)(2). Certification shall be submitted in December of each year to LEAA until such complete compliance. The yearly certification shall update the information provided under § 20.21.

*§ 20.24 State laws on privacy and security.*

Where a State originating criminal history record information provides for sealing or purging thereof, nothing in these regulations shall be construed to prevent any other State receiving such information, upon notification, from complying with the originating State's sealing or purging requirements.

§ *20.25 Penalties.*

Any agency or individual violating subpart B of these regulations shall be subject to a fine not to exceed $10,000. In addition, LEAA may initiate fund cut-off procedures against recipients of LEAA assistance.

Subpart C—Federal System and Interstate Exchange of Criminal History Record Information

§ *20.30 Applicability.*

The provisions of this subpart of the regulations apply to any Department of Justice criminal history record information system that serves criminal justice agencies in two or more states and to Federal, state and local criminal justice agencies to the extent that they utilize the services of Department of Justice criminal history record information systems. These regulations are applicable to both manual and automated systems.

§ *20.31 Responsibilities*

(a) The Federal Bureau of Investigation (FBI) shall operate the National Crime Information Center (NCIC), the computerized information system which includes telecommunications lines and any message switching facilities which are authorized by law or regulation to link local, state and Federal criminal justice agencies for the purpose of exchanging NCIC-related information. Such information includes information in the Computerized Criminal History (CCH) File, a cooperative Federal-State program for the interstate exchange of criminal history record information. CCH shall provide a central repository and index of criminal history record information for the purpose of facilitating the interstate exchange of such information among criminal justice agencies.

(b) The FBI shall operate the Identification Division to perform identification and criminal history record information functions for Federal, state and local criminal justice agencies, and for noncriminal justice agencies and other entities where authorized by Federal statute, state statute pursuant to Public Law 92–544 (86 Stat. 1115), Presidential executive order, or regulation of the Attorney General of the United States.

(c) The FBI Identification Division shall maintain the master fingerprint files on all offenders included in the NCIC/CCH File for the purposes of determining first offender status and to identify those offenders who are unknown in states where they become criminally active but known in other states through prior criminal history records.

§ *20.32 Includable offenses.*

(a) Criminal history record information maintained in any Department of Justice criminal history record information system shall include serious and/or significant offenses.

(b) Excluded from such a system are arrests and court actions limited to only, nonserious charges, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, non-specific charges of suspicion or investigation, traffic violations (except data will be included on arrests for manslaughter, driving under the influence of drugs or liquor, and hit and run). Offenses committed by juvenile offenders shall also be excluded unless a juvenile offender is tried in court as an adult.

(c) The exclusions enumerated above shall not apply to Federal manual criminal history record information collected, maintained and compiled by the FBI prior to the effective date of these Regulations.

§ *20.33 Dissemination of criminal history record information.*

(a) Criminal history record information contained in any Department of Justice criminal history record information system will be made available:

(1) To criminal justice agencies for criminal justice purposes; and

(2) To Federal agencies authorized to receive it pursuant to Federal statute or Executive order.

(3) Pursuant to Public Law 92–544 (86 Stat. 115) for use in connection with licensing or local/state employment or for other uses only if such dissemination is authorized by Federal or state statutes and approved by the Attorney General of the United States. When no active prosecution of the charge is known to be pending arrest data more than one year old will not be disseminated pursuant to this subsection unless accompanied by information relating to the disposition of that arrest.

(4) For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses.

(b) The exchange of criminal history record information authorized by paragraph (a) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies.

(c) Nothing in hese regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates.

*§ 20.34 Individual's right to access criminal history record information.*

(a) Any individual, upon request, upon satisfactory verification of his identity by fingerprint comparison and upon payment of any required processing fee, may review criminal history record information maintained about him in a Department of Justice criminal history record information system.

(b) If, after reviewing his identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections or updating of the alleged deficiency, he must make application directly to the contributor of the questioned information. If the contributor corrects the record, it shall promptly notify the FBI and, upon receipt of such a notification, the FBI will make any changes necessary in accordance with the correction supplied by the contributor of the original information.

*§ 20.35 National Crime Information Center Advisory Policy Board.*

There is established an NCIC Advisory Policy Board whose purpose is to recommend to the Director, FBI, general policies with respect to the philosophy, concept and operational principles of NCIC, particularly its relationships with local and state systems relating to the collection, processing, storage, dissemination and use of criminal history record information contained in the CCH File.

(a)(1) The Board shall be composed of twenty-six members, twenty of whom are elected by the NCIC users from across the entire United States and six who are appointed by the Director of the FBI. The six appointed members, two each from the judicial, the corrections and the prosecutive sectors of the criminal justice community, shall serve for an indeterminate period of time. The twenty elected members shall serve for a term of two years commencing on January 5th of each odd numbered year.

(2) The Board shall be representative of the entire criminal justice communuity at the state and local levels and shall include representation from law enforcement, the courts and corrections segments of this community.

(b) The Board shall review and consider rules, regulations and procedures for the operation of the NCIC.

(c) The Board shall consider operational needs of criminal justice agencies in light of public policies, and local, state and Federal statutes and these Regulations.

(d) The Board shall review and consider security and privacy aspects of the NCIC system and shall have a standing Security and Confidentiality Committee to provide input and recommendations to the Board concerning security and privacy of the NCIC system on a continuing basis.

(e) The Board shall recommend standards for participation by criminal justice agencies in the NCIC system.

(f) The Board shall report directly to the Director of the FBI or his designated appointee.

(g) The Board shall operate within the purview of the Federal Advisory Committee Act, Public Law 92–463, 86 Stat. 770.

(h) The Director, FBI, shall not adopt recommendations of the Board which would be in violation of these Regulations.

*§ 20.36 Participation in the Computerized Criminal History Program.*

(a) For the purpose of acquiring and retaining direct access to CCH File each criminal justice agency shall execute a signed agreement with the Director, FBI, to abide by all present rules, policies and procedures of the NCIC, as well as any rules, policies and procedures hereinafter approved by the NCIC Advisory Policy Board and adopted by the NCIC.

(b) Entry of criminal history record information into the CCH File will be accepted only from an authorized state or Federal criminal justice control terminal. Terminal devices in other authorized criminal justice agencies will be limited to inquiries.

*§ 20.37 Responsibility for accuracy, completeness, currency.*

It shall be the responsibility of each criminal justice agency contributing data to any Department of Justice criminal history record information system to assure that information on individuals is kept complete, accurate and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred.

*§ 20.38 Sanction for noncompliance.*

The services of Department of Justice criminal history record information systems are subject to cancellation in regard to any agency or entity which fails to comply with the provisions of Subpart C.

EDWARD H. LEVI,
*Attorney General.*

May 15, 1975.

RICHARD W. VELDE,
*Administrator, Law Enforcement Assistance Administration.*

May 15, 1975.

APPENDIX—COMMENTARY ON SELECTED SECTIONS OF THE REGULATIONS ON CRIMINAL HISTORY RECORD INFORMATION SYSTEMS

*Subpart A*—*§ 20.3(b)*. The definition of criminal history record information is intended to include the basic offender-based transaction statistics/computerized criminal history (OBTS/CCH) data elements. If notations of an arrest, disposition, or other formal criminal justice transactions occur in records other than the traditional "rap sheet" such as arrest reports, any criminal history record information contained in such reports comes under the definition of this subsection.

The definition, however, does not extend to other information contained in criminal justice agency reports. Intelligence or investigative information (e.g. suspected criminal activity, associates, hangouts, financial information, ownership of property and vehicles) is not included in the definition of criminal history information.

*§ 20.3(c)*. The definitions of criminal justice agency and administration of criminal justice of 20.3(c)(d) must be considered together. Included as criminal justice agencies would be traditional police, courts, and corrections agencies as well as subunits of noncriminal justice agencies performing a function of the administration of criminal justice pursuant to Federal or State statute or executive order. The above subunits of non-criminal justice agencies would include for example, the Office of Investigation of the U.S. Department of Agriculture which has as its principal fuction the collection of evidence for criminal prosecutions of fraud. Also included under the definition of criminal justice agency are umbrella-type administrative agencies supplying criminal history information services such as New York's Division of Criminal Justice Services.

*§ 20.3(e)*. Disposition is a key concept in the section 524(b) of the Act and in § 20.21(a)(1) and § 20.21(b)(2). It, therefore, is defined in some detail. The specific dispositions listed in this subsection are examples only and are not to be construed as excluding other unspecified transactions concluding criminal proceedings within a particular agency.

*Subpart B*—*§ 20.20(a)*. These regulations apply to criminal justice agencies receiving Safe Streets funds for manual or automated systems subsequent to July 1, 1973. In the hearings on the regulations, a number of those testifying challenged LEAA's authority to promulgate regulations for manual systems by contending that section 524(b) of the Act governs criminal history information contained in automated systems.

The intent of section 524(b), however, would be subverted by only regulating automated systems. Any agency that wished to circumvent the regulations would be able to create duplicated manual files for purposes contrary to the letter and spirit of the regulations.

Regulations of manual systems, therefore, is authorized by section 524(b) when coupled with Section 501 of the Act which authorizes the Administrtion to establish rules and regulations "necessary to the exercise of its functions * * *."

The Act clearly applies to all criminal history record information collected, stored, or disseminated with LEAA support subsequent to July 1, 1973.

*§ 20.20(b)(c)*. Section 20.20(b)(c) exempts from regulations certain types of records vital to the apprehension of fugitives, freedom of the press, and the public's right to know.

Section 20.20(b)(ii) attempts to deal with the problem of computerized police blotters. In some local jurisdictions, it is apparently possible for private individuals and/or newsmen upon submission of a specific name to obtain through a computer search of the blotter a history of a person's arrests. Such files create a partial criminal history data bank potentially damaging to individual privacy, especially since they do not contain final dispositions. By requiring that such records be accessed solely on a chronological basis, the regulations limit inquiries to specific time periods and discourage general fishing expeditions into a person's private life.

Subsection 20.20(c) recognizes that announcements of ongoing developments in the criminal justice process should not be precluded from public disclosure. Thus announcements of arrest, convictions, new developments in the course of an investigation may be made within a few days of their occurrence. It is also permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. Thus, if a question is raised: "Was X arrested by your agency on January 3, 1952" and this can be confirmed or denied by looking at one of the records enumerated in subsection (b) above, then the criminal agency may respond to the inquiry.

*§ 20.21.* Since privacy and security considerations are too complex to be dealt with overnight, the regulations require a State plan to assure orderly progress toward the objectives of the Act. In response to requests of those testifying on the draft regulations, the deadline for submission of the plan was set at 180 days. The kind of planning document anticipated would be much more concise than, for example, the State's criminal justice comprehensive plan.

The regulations deliberately refrain from specifying who within a State should be responsible for preparing the plan. This specific determination should be made by the Governor.

*§ 20.21(a)(1).* Section 524(b) of the Act requires that LEAA insure criminal history information be current and that, to the maximum extent feasible, it contain disposition as well as current data.

It is, however, economically and administratively impractical to maintain complete criminal histories at the local level. Arrangements for local police departments to keep track of dispositions by agencies outside of the local jurisdictions generally do not exist. It would, moreover, be bad public policy to encourage such arrangements since it would result in an expensive duplication of files.

The alternatives to locally kept criminal histories are records maintained by a central State repository. A central State repository is a State agency having the function pursuant to statute or executive order of maintaining comprehensive statewide criminal history record information files. Ultimately, through automatic data processing the State level will have the capability to handle all requests for in-State criminal history information.

Section 20.21(a)(1) is written with a centralized State criminal history repository in mind. The first sentence of the subsection states that complete records should be retained at a central State repository. The word "should" is permissive; it suggests but does not mandate a central State repository.

The regulations do require that States establish procedures for State and local criminal justice agencies to query central State repositories wherever they exist. Such procedures are intended to insure that the most current criminal justice information is used.

As a minimum, criminal justice agencies subject to these regulations must make inquiries of central State repositories whenever the repository is capable of meeting the user's request within a reasonable time. Presently, comprehensive records of an individual's transactions within a State are maintained in manual files at the State level, if at all. It is probably unrealistic to expect manual systems to be able immediately to meet many rapid-access needs of police and prosecutors. On the other hand, queries of the State central repository for most noncriminal justice purposes probably can and should be made prior to dissemination of criminal history record information.

*§ 20.21(b).* The limitations on dissemination in this subsection are essential to fulfill the mandate of section 524(b) of the Act which requires the Administration to assure that the "privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes." The categories for dissemination established in this section reflect suggestions by hearing witnesses and respondents submitting written commentary.

§ *20.21(b)(2)*. This subsection is intended to permit public or private agencies to have access to criminal history record information where a statute or executive order:

(1) Denies employment, licensing, or other civil rights and privileges to persons convicted of a crime;

(2) Requires a criminal record check prior to employment, licensing, etc.

The above examples represent statutory patterns contemplated in drafting the regulations. The sine qua non for dissemination under this subsection is statutory reference to criminal conduct. Statutes which contain requirements and/or exclusions based on "good moral character" or "trust worthiness" would not be sufficient to authorize dissemination.

The language of the subsection will accommodate Civil Service suitability investigations under Executive Order 10450, which is the authority for most investigations conducted by the Commission. Section 3(a) of 10450 prescribes the minimum scope of investigation and requires a check of FBI fingerprint files and written inquiries to appropriate law enforcement agencies.

§ *20.21(b)(3)*. This subsection would permit private agencies such as the Vera Institute to receive criminal histories where they perform a necessary administration of justice function such as pretrial release. Private consulting firms which commonly assist criminal justice agencies in information systems development would also be included here.

§ *20.21(b)(4)*. Under this subsection, any good faith researchers including private individuals would be permitted to use criminal history record information for research purposes. As with the agencies designated in § 20.21(b)(3) researchers would be bound by an agreement with the disseminating criminal justice agency and would, of course, be subject to the sanctions of the Act.

The drafters of the regulations expressly rejected a suggestion which would have limited access for research purposes to certified research organizations. Specifically "certification" criteria would have been extremely difficult to draft and would have inevitably led to unnecessary restrictions on legitimate research.

Section 524(a) of the Act which forms part of the requirements of this section states:

"Except as provided by Federal law other than this title, no officer or employee of the Federal Government, nor any recipient of assistance under the provisions of this title shall use or reveal any research or statistical information furnished under this title by any person and identifiable to any specific private person for any purpose other than the purpose for which it was obtained in accordance with this title. Copies of such information shall be immune from legal process, and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceedings."

LEAA anticipates issuing regulations pursuant to Section 524(a) as soon as possible.

§ *20.21(b)(5)*. Dissemination under this section would be permitted not only in cases of investigations of employment suitability, but also investigations relating to clearance of individuals for access to information which is classified pursuant to Executive Order 11652.

§ *20.21(c)(1)*. "Active prosecution pending" would mean, for example, that the case is still actively in process, the first step such as an arraignment has been taken and the case docketed for court trial. This term is not intended to include any treatment alternative-type program which might defer prosecution to a later date. Such a deferral prosecution is a disposition which should be entered on the record.

§ *20.21(c)(3)*. Presently some employers are circumventing State and local dissemination restrictions by requesting applicants to obtain an official certification of no criminal record. An employer's request under the above circumstances gives the applicant the unenviable choice of invasion of his privacy or loss of possible job opportunities. Under this subsection routine certifications of no record would no longer be permitted. In extraordinary circumstances, however, an individual could obtain a court order permitting such a certification.

§ *20.21(c)(4)*. The language of this subsection leaves to the States the question of who among the agencies and individuals listed in § 20.21(b) shall actually receive criminal records. Under these regulations a State could place a total ban on dissemination if it so wished.

§ *20.21(d)*. Non-criminal justice agencies will not be able to receive records of juveniles unless the language or statute or Federal executive order specifies that

juvenile records shall be available for dissemination. Perhaps the most controversial part of this subsection is that it denies access to records of juveniles by Federal agencies conducting background investigations for eligibility to classified information under existing legal authority.

§ *20.21(e)*. Since it would be too costly to audit each criminal justice agency in most States (Wisconsin, for example, has 1075 criminal justice agencies) random audits of a "representative sample" of agencies are the next best alternative. The term "representative sample" is used to insure that audits do not simply focus on certain types of agencies.

§ *20.21(f)(2)*. In the short run, dedication will probably mean greater costs for State and local governments. How great such costs might be is dependent upon the rapidly advancing state of computer technology. So that there will be no serious hardship on States and localities as a result of this requirement, § 20.23 provides that additional time will be allowed to implement the dedication requirement. For example, where local systems now in place contain criminal history information of only that State, used purely for intrastate purposes, in a shared environment, consideration will be given to granting extensions of time under this provision.

§ *20.21(f)* (*5*), (*8*). "Direct access" means that any non-criminal agency authorized to receive criminal justice data must go through a criminal justice agency to obtain information.

§ *20.21(g)(1)*. A "challenge" under this section is an oral or written contention by an individual that his record is inaccurate or incomplete; it would require him to give a correct version of his record and explain why he believes his version to be correct. While an individual should have access to his record for review, a copy of the record should ordinarily only be given when it is clearly established that it is necessary for the purpose of challenge.

The drafters of the subsection expressly rejected a suggestion that would have called for a satisfactory verification of identity by fingerprint comparison. It was felt that states ought to be free to determine other means of identity verification.

§ *20.21(g)(5)*. Not every agency will have done this in the past, but henceforth adequate records including those required under § 20.21(e) must be kept so that notification can be made.

§ *20.21(g)(6)*. This section emphasizes that the right to access and review extends only to criminal history information and does not include other information such as intelligence or treatment data.

§ *20.22(a)*. The purpose for the certification requirement is to initiate immediate compliance with these regulations wherever possible. The term "maximum extent feasible" acknowledges that there are some areas such as the completeness requirement which create complex legislative and financial problems.

NOTE: In preparing the plans required by these regulations, States should look for guidance to the following documents: National Advisory Commission on Criminal Justice Standards and Goals, Report on the Criminal Justice System; Project SEARCH: Security and Privacy Considerations in Criminal History Information Systems, Technical Report #2; Project SEARCH: A Model State Act for Criminal Offender Record Information, Technical Memorandum #3; and Project SEARCH: Model Administrative Regulations for Criminal Offender Record Information, Technical Memorandum #4.

*Subpart C*—§ *20.31*. Defines the criminal history record information system operated by the Federal Bureau of Investigation. Each state having a record in the Computerized Criminal History (CCH) file must have a fingerprint card on file in the FBI Identification Division to support the CCH record concerning the individual.

Paragraph b is not intended to limit the identification services presently performed by the FBI for Federal, state and local agencies.

§ *20.32*. The grandfather clause contained in the third paragraph of this Section is designed, from a practical standpoint, to eliminate the necessity of deleting from the FBI's massive files the non-includable offenses which were stored prior to February, 1973.

In the event a person is charged in court with a serious or significant offense arising out of an arrest involving a non-includable offense, the non-includable offense will appear in the arrest segment of the CCH record.

§ *20.33*. Incorporates the provisions of a regulation issued by the FBI on June 16, 1974, limiting dissemination of arrest information not accompanied by disposition information outside the Federal government for non-criminal justice purposes. This regulation is cited in 28 CFR 50.12.

§ *20.34*. The procedures by which an individual may obtain a copy of his manual identification record are particularized in 28 CFR 16.30–34.

The procedures by which an individual may obtain a copy of his Computerized Criminal History record are as follows:

If an individual has a criminal record supported by fingerprints and that record has been entered in the NCIC CCH File, it is available to that individual for review, upon presentation of appropriate identification, and in accordance with applicable state and Federal administrative and statutory regulations.

Appropriate identification includes being fingerprinted for the purpose of insuring that he is the individual that he purports to be. The record on file will then be verified as his through comparison of fingeprints.

*Procedure.* 1. All requests for review must be made by the subject of his record through a law enforcement agency which has access to the NCIC CCH File. That agency within statutory or regulatory limits can require additional identification to assist in securing a positive identification.

2. If the cooperating law enforcement agency can make an identification with fingerprints previously taken which are on file locally and if the FBI identification number of the individual's record is available to that agency, it can make an on-line inquiry of NCIC to obtain his record on-line or, if it does not have suitable equipment to obtain an on-line response, obtain the record from Washington, D.C., by mail. The individual will then be afforded the opportunity to see that record.

3. Should the cooperating law enforcement agency not have the individual's fingerprints on file locally, it is necessary for that agency to relate his prints to an existing record by having his identification prints compared with those already on file in the FBI or, possibly, in the State's central identification agency.

4. The subject of the requested record shall request the appropriate arresting agency, court, or correctional agency to initiate action necessary to correct any stated inaccuracy in his record or provide the information needed to make the record complete.

§ *20.36.* This section refers to the requirements for obtaining direct access to the CCH file. One of the requirements is that hardware, including processor, communications control and storage devices, to be utilized for the handling of criminal history data must be dedicated to the criminal justice function.

§ *20.37.* The 120-day requirement in this section allows 30 days more than the similar provision in Subpart B in order to allow for processing time which may be needed by the states before forwarding the disposition to the FBI.

[FR Doc. 75-13197 Filed 5-19-75;8:45 am]

---

[Order No. 602-75]

## PART 50—STATEMENTS OF POLICY

### RELEASE OF INFORMATION BY PERSONNEL OF THE DEPARTMENT OF JUSTICE RELATING TO CRIMINAL AND CIVIL PROCEEDINGS

This order amends the Department of Justice guidelines concerning release of information by personnel of the Department of Justice relating to criminal and civil proceedings by deleting the provision permitting disclosure of criminal history record information on request.

By virtue of the authority vested in me as Attorney General of the United States, § 50.2(b)(4) of Chapter I, Title 28 of the Code of Federal Regulations is amended to read as follows:

§ *50.2 Release of information by personnel of the Department of Justice relating to criminal and civil proceedings.*

* * * * * * *

(b) * * *

* * * * * * *

(4) Personnel of the Department shall not disseminate any information concerning a defendant's prior criminal record.

* * * * * * *

May 15, 1975.

EDWARD H. LEVI, *Attorney General.*

[FR Doc. 75-13198 Filed 5-19-75;8:45 am]

[From the New York Times, July 15, 1975]

## FBI, for First Time, To Expunge Record of Legal Federal Arrest

(By Linda Charlton)

Washington, July 14—The shadow that had darkened the life of a respected school administrator for 24 years has been lifted by a recent agreement of the Federal Bureau of Investigation to expunge her arrest record—the first time this has been done in a legal, Federal arrest.

The F.B.I. "stipulation," or binding agreement, was signed June 24, after a suit was filed Sept. 23, 1974, in United States District Court here by the American Civil Liberties Union on behalf of the woman, identified only as "Jane Doe."

Previously, according to John H. Shattuck, the A.C.L.U. lawyer who handled the case, the F.B.I. has agreed to expunge legal arrest records if they are on state charges and such erasure is required by state statutes when charges are dismissed. Records of arrests later ruled to be illegal—such as those of the 13,000 May day demonstrators in 1971—have also been expunged.

The stipulation in the case, Mr. Shattuck said, sets a precedent in the non-technical sense that it will "make it difficult for the F.B.I. to take a different position with respect to other people" in similar circumstances.

### 1947 ARREST WITH HUSBAND

In the complaint filed last September, the plaintiff, Jane Doe, is described as "a senior education official in the public school system of a major American city" who has "published widely in professional journals and has been awarded certificates of appreciation from governor of a state in which she has served periodically as an educational consultant."

But back in 1947, when she was 20 years old, she married the pseudosymous "James Poe," and four years later she and her former husband were arrested on charges of transporting stolen property in interstate commerce. The charges against her were subsequently dismissed when it was shown that James Poe had concealed from her "the fact that he had stolen property and transported it in interstate commerce during the trip on which she had accompanied him."

James Poe was convicted and sentenced; in 1954, Jane Poe obtained a statutory annulment of her marriage on the grounds that he had concealed not only this crime but also his prior criminal record.

Since then, she has remarried, obtained her doctorate, and had, the complaint states, "an extraordinarily useful and productive career."

But the record of the arrest remained in the F.B.I.'s files, and the complaint alleges that "the life of the plaintiff has been continually overshadowed by her well-grounded apprehension that the record of her seizure will be exposed or disseminated by the defendants, causing her loss of employment and professional stature."

### FEAR OF BLACKMAIL CITED

She has bypassed opportunities for promotion from fear that the record will be disclosed, the complaint says, and has been in "continual jeopardy" of dismissal, loss of pension rights, or even blackmail.

The stipulation to which both the F.B.I. and Jane Doe agreed states that the bureau will physically destroy her record, "together with any record information derived therefrom," and will remove her fingerprints and name card within 30 days.

The F.B.I. will also notify the appropriate offices in Los Angeles and Detroit both of which have her fingerprints on file, to destroy them.

Within 30 additional days, the bureau will notify all agencies to which the record has been sent to destroy these as well. The stipulation notes that the agreement "does not represent a binding precedent or policy."

Jane Doe, described as being at "a crucial point in her career," can now proceed without fear of the past. "She really feels rejuvenated, is the way she put it to me," Mr. Shattuck said.

## CORRESPONDENCE

National Cargo Security Council,
*Washington, D.C., July 22, 1975.*

Hon. John V. Tunney,
*Chairman, Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, Washington, D.C.*

Dear Mr. Chairman: We understand that your Subcommittee is currently considering S. 2008, legislation to restrict the compilation and dissemination of criminal records.

This is a question which significantly affects the subject of transportation cargo security, which has been defined by both the Congress and the Executive Branch to be a problem of national scope and importance. Access by the transportation industry, under appropriate controls and safeguards to protect the rights of individuals, is an important component of viable and effective cargo security programs.

The National Cargo Security Council was created in 1971 under the aegis of the Transportation Association of America to facilitate improvement in cargo security policies and programs. This action was paralleled by concurrent establishment of the governmental Interagency Committee on Transportation Security (ICOTS), with which the Council has worked closely over the intervening years. The Council is comprised of members representing all facets of the transportation industry—transport labor unions, insurors, importers, users and carriers of all modes—who share an interest in bringing about reduction of the problems of theft and pilferage which plague this industry.

It has been estimated that at least $1 billion per year in merchandise is lost due to criminal misappropriation of goods in transit. A certain proportion of this loss results from such activities as truck hijackings, burglary, armed robbery and other crimes perpetrated by "outsiders." However, although these crimes receive much greater publicity, it is also estimated by those knowledgeable in this area, including the U.S. Department of Transportation, that the bulk of such criminal losses are "inside" crimes; that is, they represent theft and pilferage by individuals in the employ of the transportation industry whose opportunities for crime arise as a product of their employment.

The transportation industry is working diligently, through the Council, through other organizations and on a company-by-company basis, to bring about improvement in transportation cargo security procedures and practices. Because the preponderance of cargo theft and pilferage is perpetrated by those in the employ of the industry, a major portion of this effort must necessarily be directed toward improvement of employee screening programs. These programs can be effectively implemented only if transportation companies can gain access to criminal records information regarding prospective employees.

For this reason, the Council believes it of major importance that legislative obstacles not be interposed to reasonable development of this data. We believe this information can be of considerable benefit in conjunction with *bona fide* cargo security programs to reduce the incidence of theft and pilferage of transportation cargoes.

To safeguard the rights and privacy of individuals, it is the Council's proposal that this information (1) cover only records of convictions, forfeitures and *nolo contendere* pleas; (2) be limited to a past period of seven years prior to the date of inquiry, and (3) be made available only on written authorization of the individual whose records are sought. We stress that we are seeking in this regard only information which is currently a matter of public record in the court in which the action took place; our concern is that, if the transportation industry is barred from accessing more centralized data sources as they are developed, the multiplicity of jurisdictions in this country and the need for performing security checks in each such jurisdiction to develop a complete record, will continue to pose major obstacles to cargo security programs, to the detriment of the national industry/government cooperative effort to bring about improvement in this field. We believe such a result would be an inappropriate byproduct of this legislation, unnecessarily impeding, rather than furthering, national goals.

Accordingly, we hope that your Subcommittee will, in considering this legislation, give full recognition to the needs of the transportation industry in this

regard by providing for availability of criminal records information subject to the conditions and safeguards described above. In this way we believe national objectives concerning transportation cargo security can be better realized without doing violence to any individual rights under the Constitution and laws of the nation.

Thank you very much for your attention. We would like to request that this letter be made part of the record on this legislation.

Sincerely,

HAROLD F. HAMMOND.

---

STATE OF MICHIGAN,
OFFICE OF THE GOVERNOR,
*Lansing, July 29, 1975.*

Hon. JOHN TUNNEY,
*U.S. Senator, Dirksen Senate Office Building,*
*Washington, D.C.*

DEAR SENATOR TUNNEY: I am pleased to take this opportunity to lend my support to S. 2008, which would regulate collection and dissemination of criminal justice information. I firmly believe that government should accelerate its efforts to make protection of personal privacy in the United States a reality. The adoption of S. 2008 would be a significant step in that direction.

All of us are aware of the tremendous strides which have been made in the past few years in the technical capacity to compile, house, and disseminate criminal justice information. These techniques represent a valuable if not essential law enforcement tool. However, the resulting aggregation of information in centralized records centers at the state, regional, and national levels creates potentials for abuse which did not exist when we relied on fragmatized, locally held records systems. At the same time, our advanced computer technology has itself given us new tools with which to provide tighter security controls if we will only use them. But because our criminal justice information systems are no longer confined within state borders, I believe it is imperative for the federal government to enact minimum operating standards for all jurisdictions in the country.

While recognizing the need for federal legislation, however, I think it is equally important for Congress to recognize the basic interest of states with respect to their law enforcement responsibilities. Law enforcement is primarily a function of state and local agencies. It is these agencies which compile the greatest portion of criminal justice information and also have the most frequent need for access to it. I am especially pleased that S. 2008 recognizes the interests of the states in several of its provisions, particularly in section 301 pertaining to the composition of the Commission on Criminal Justice Information.

One aspect of the bill which does concern me is the effect it will have on criminal history records currently being maintained by law enforcement agencies. It is not clear to me whether the bill's provisions will be limited to prospective applications or whether its requirements will be uniformly applicable to all records in existence prior to enactment. While I would certainly agree that information on hand prior to enactment of S. 2008 should be subject to the same dissemination and use restrictions as those applied to records compiled after enactment, I would be opposed to requiring immediate updating with respect to existing records.

Such a requirement, I believe, would be both costly and unnecessary. Section 208(a)(4), for example, requires the purging of criminal history record information in any case in which prosecution has not resulted. If applied retroactively, this provision would require law enforcement agencies to search all existing records in order to determine which entries are subject to the purging requirement. This would obviously result in tremendous burdens to state and local governments. I believe the bill ought to clearly indicate that revision of existing records need not be undertaken until a particular file is next requested for use or for review by the person identified in it. In either of these events, of course, the file ought to be carefully screened for accuracy and compliance with the law before it is made available to any authorized person or agency.

The need for enactment of an effective, balanced criminal justice information bill has been recognized for several years. I am in complete agreement with your belief that this issue merits prompt Congressional attention, and I share your hope for early enactment of this bill.

Warm personal regards.

Sincerely,

WILLIAM G. MILLIKEN, *Governor.*

STATE OF NEW JERSEY,
OFFICE OF THE GOVERNOR,
*Trenton, July 30, 1975.*

Hon. JOHN V. TUNNEY,
*Los Angeles, Calif.*

DEAR SENATOR TUNNEY: I am pleased to learn that you have submitted to Deputy Attorney General Tyler requests for information on the FBI's criminal justice information proposal for inclusion in your sub-committee's hearing record on S. 2008.

The Department of Justice proposed regulations in the Federal Register May 20, 1975 to require that states store criminal justice histories in dedicated computer facilities.

This proposal has generated substantial opposition among the Nation's Governors.

At the annual meeting of the National Governors' Conference, the Committee on Crime Reduction and Public Safety, which I chair, expressly affirmed a policy statement which provides that the states shall "determine whether information should be stored in a shared or dedicated facility". The full Governors' Conference endorsed this policy position at its plenary session.

This week, at a meeting of the Executive Committee of the National Governors' Conference, Governor Bond of Missouri raised, in the strongest possible terms his continuing opposition to the FBI proposal.

I urge your Committee to investigate whether dedication of computer facilities and personnel at enormous cost to many state governments enhances in any way the security and privacy of criminal justice information. Unless it can be shown that dedication is necessary for the confidentiality of these records, I believe the federal government should not preempt the state's discretion in this matter.

Sincerely,

BRENDAN T. BYRNE, *Governor.*

---

AMERICAN NEWSPAPER PUBLISHERS ASSOCIATION,
*Washington, D.C., August 1, 1975.*

Hon. JOHN V. TUNNEY,
*Chairman, Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, Washington, D.C.*

DEAR MR. CHAIRMAN: In furtherance of your letter of July 9, concerning S 2008, I wish to thank you for this opportunity to address the problems involving the press as affected by this proposed legislation. This statement is submitted for inclusion in the record of hearings on S 2008 conducted by your Subcommittee on July 15 and 16.

The American Newspaper Publishers Association is joined in this presentation by the American Society of Newspaper Editors, the National Newspaper Association and the Associated Press Managing Editors Association. A brief description of these four associations follows.

The ANPA is the national trade association of daily newspapers with a membership of more than 1100 daily newspapers representing more than ninety percent of the total daily and Sunday newspaper circulation in the United States. The ASNE is a nationwide professional organization of more than 800 persons holding positions as directing editors of daily newspapers throughout the United States. The NNA is a trade association representing more than 5500 weekly and 950 small city daily newspapers throughout the United States with a total circulation of more than 40 million. The APME is an association which represents 500 managing editors of large and small newspapers across the country.

In submitting this statement on behalf of these four major press related organizations, we would like to call your attention to the fact that we recognize that the Subcommittee has seen fit, in the present version of S 2008, to rectify some of the objections we earlier expressed to S 2963 and S 2964 which had been introduced into the prior Congress as predecessor bills to S 2008.

Despite these changes, however, S 2008 fails to address the principal objections we have long held concerning this proposed legislation.

On March 13, 1974, representatives of the press testified before this Subcommittee at the initial hearings on S 2963 and S 2964. At that time, we stated our support for the effort being made to improve the accuracy and efficiency of handling of criminal justice information. We strongly urged upon the Subcommittee the view that this legislation presented a clear danger to the continued

free flow of proper information to the public in the area of criminal justice, and we objected to any extensive conversion of essentially public records to private records.

Unfortunately, S 2008 as drafted accomplishes the very thing we warned against. It would effectively shut off the public to the great bulk of criminal justice information. It would make the operation of the criminal justice systems virtually unaccountable to the public. The intention of this bill is laudable: to further the protection of individual privacy. The result is lamentable: the placement of the public's business behind locked doors.

This is a clear contravention of the concept of openness in government which the Congress so emphatically endorsed just last year through enactment of the Freedom of Information Act amendments. We believe that recent events in our national life have made it clear that the public interest in, and support for, openness in government and freedom of information are every bit as strong and compelling as the concern for individual privacy. This, however, is a concept that S 2008 has not recognized.

Under this bill, for example, a person who has a past record of bribery convictions could be appointed to a city position in which he is responsible for awarding contracts through sealed bids. Shouldn't the mayor who appoints him and the public who pays him have the right to know about that bribery conviction? As drafted, S. 2008 would prevent the mayor and the public from access to this information, a result clearly not in the public interest.

And how about the police chief or prosecutor who use their positions to protect criminals from prosecution because of graft, friendship or other improper reasons? Doesn't the public have the right to know this? Under S. 2008 they would not! There are numerous other examples that could be offered, but the point is clear.

In addition to substantive problems, S 2008 contains some confusing and contradictory language. For example:

Section 208(a) does not make clear that it does not apply to the records detailed in Section 103(c). Section 103(c) states that the Act does not apply to court records. Yet, Section 208(a) requires criminal justice agencies, which include the courts, to adopt procedures for sealing their records.

Section 209(d) does not even parse out as a sentence. We specifically mention this because obviously we cannot make any substantive comments on same as there is no way for us to know whether it affects the press or not.

The consequences of Section 314 on the Privacy Act of 1974 are far from clear.

The failings of this bill are so serious that we regretfully believe that we must recommend to our members nationally that the bill in its present form be opposed to the fullest extent.

Nevertheless, we recognize the importance of protecting the right to privacy and of balancing that right against the necessity for a free flow of information about public matters to the people.

In an effort to be of assistance to the Subcommittee we now, ad seriatim, suggest language changes which would establish that balance and thereby make S 2008 more acceptable to the press and, we believe, of far greater service to the interest of the general public and to government.

Section 103(c) is intended to maintain the public nature of certain records such as police blotters and court records. In many jurisdictions these are public records as a matter of custom and tradition and not necessarily as a matter of statute.

Section 103(c)(1) as drafted, does not reflect the statutory intent that access to police blotters be maintained regardless of whether that access is a matter of statute or a matter of custom. Specifically, we would recommend that Section 103(c)(1) be changed to place a semicolon after the word "name" on line 7 of page 7 and delete the language "and required to be made public."

Similarly, Section 103(c)(2) does not clearly reflect the concept that court records of public criminal proceedings should be accessible to the public. We would recommend that this section be rewritten into two sections; one dealing with court records of public criminal proceedings and the other dealing with official records of pardons or paroles. The new sections would read:

"103(c)(2) Court records of public criminal proceedings or any index thereto organized and accessible by date or by docket or file number, or organized and accessible by name;

"103(c)(3) Official records of pardons or paroles or any index thereto organized and accessible by date or by docket or file number, or organized and acces-

sible by name, so long as such index contains no other information than a cross reference to the original pardon or parole records by docket or file number;"

Sections 103(c) (3), (4), (5), and (6) would be changed respectively to Sections 103(c) (4), (5), (6), and (7).

The press is concerned, as is the Subcommittee, with maintaining the highest standards of accuracy in reporting criminal justice information to the public. It was to this end that section 203(h) was included. This section permits a criminal justice agency to confirm specific inquiries by members of the press. As drafted, however, this section would appear to limit the criminal justice agency to confirming prior arrest record or criminal record information only if the request is based on information obtained from a foreign government or international police agency. We would therefore recommend that Section 203(h) be changed to insert a period after the word "date" on page 14, line 3. The remaining language in that section should be deleted.

Section 206(a). This section appears to work at cross-purposes to Section 103(c) (1) which maintains the public nature of police blotters. Section 206(a), however, requires that an inquiry for information relating to an individual be based upon identification of that individual by name *and* other personal information. We would recommend that the word "and" on page 17, line 3, be deleted and the word "or" be substituted.

At this point we place particular emphasis on our effort to cure the apparent imbalance between the individual's right of privacy and the public's right to an open government as it appears in Section 208 of the bill as drafted. The course we recommend is to limit the operation of this section to records pertaining to offenses other than felonies. In this way, an individual who committed a relatively less severe offense would not have a criminal record follow him throughout his life, yet the public would still have access to information pertaining to serious crimes. It should be noted that Section 208 would still result in sealing of records pertaining to a wide range of offenses including petty theft, shoplifting, simple assaults and possession of small amounts of marijuana, as examples.

Specifically in Section 208(a)(1) the phrase "relating to an offense other than a felony" should be inserted after the word "information" on page 19, line 13. Similarly, the phrase "other than a felony" should be inserted after the word "offense" on page 19, line 16. The phrase "relating to an offense other than a felony" should be inserted after the word "information" on page 19, line 23. The phrase "relating to an offense other than a felony" should be substituted for the phrase "in any case" on page 20, line 4. The words "seek an indictment" on page 20, line 7, should be deleted.

Section 208 presents another serious problem. As drafted, this section would permit a criminal justice agency to adopt even more stringent regulations than those contained in S. 2008 once the bill becomes law. To prevent this, we urge that the words "at a minimum" on page 19, line 11, be deleted.

This section also raises a potential internal conflict in the operation of the statute. As drafted, Section 208(a) permits a criminal justice agency to purge or seal certain records. Yet Section 208(b) provides for sealed records to be opened under certain circumstances. Obviously, if the agency purged the record instead of sealing it, it would no longer have a record to open in accord with the provisions of 208(b). We would therefore recommend that the words "or purging" be deleted from page 19, line 12; page 19, line 15; page 19, line 22; and that the word "purging" page 20, line 3, be deleted and the word "sealing" be substituted for it.

Section 301(a). We are concerned that the private citizens to be appointed to the proposed Commission on Criminal Justice Information by the President need not have background or expertise in the area of freedom of information or constitutional law relating to the press. To make certain that members of the Commission have expertise in all the areas of law with which they will have to deal, we recommend the following change: delete the comma after the word "privacy" on page 26, line 14, and insert instead a semicolon. Delete the words "constitutional law" on line 15 and substitute for them the words "freedom of information law; constitutional law, including specifically freedom of the press;".

The Subcommittee must recognize that in an effort to reach a compromise we are endeavoring to emphasize the role of the press in its traditional fourth estate, watchdog status as the reporter of governmental actions to the people. The comments that have preceded this conclusion should be taken in that spirit. It should be recognized that this is not in the press' self-interest, but in the interest of the public and in the interest of maintaining a watchful eye on those areas of

government which are critical to the maintenance of our form of government, namely, the police, the prosecutorial agencies and the courts. It is an unquestionable fact that democratic government ceases when the press is muzzled. It is another unquestionable fact that once the press is muzzled, the judicial and other criminal justice functions of a country cease to work in behalf of the people of the country. A fettered press is a fettered public!

With the foregoing in mind, we were surprised by the testimony given to the Subcommittee on July 16 by the American Civil Liberties Union. The ACLU laid claim to "a record unmatched by anyone in defending freedom of the press." It then proceeded to argue against the public's interest by attacking the press for expressing reservations over the manner in which this proposed legislation would deny the public access to vital information in the criminal justice arena. We would remind the ACLU of the danger inherent in separating the watchdog role of the press from the public's own interest in open government. Too often in these days, as has begun to be noted by some of our most eminent jurists, the plea for privacy and individual protection of the criminal has been carried on to the detriment of the protection of a great majority of our nation who have not committed crimes.

We have chosen this course of attemping to improve this proposed legislation rather than simply opposing its entirety because of our belief that it is the Congress, through responsible and carefully considered legislation, which should balance the interests in privacy and openness rather than executive agencies through adoption of regulations such as those implemented on June 19 by the Law Enforcement Assistance Administration of the Department of Justice. Even though these have been in effect only since June 19, we are already receiving ominous reports. Judges in one state have stated that they will no longer recite a convicted person's record at the time of sentencing because of the LEAA regulations. This has been a traditional function of the courts in order to explain the severity or leniency of their sentences. The absence of this information deprives the public of the means for making value judgments as to the efficacy of judgments by the courts. Whether they like it or not, the Courts are just as much the servant of the people as are the executive and legislative branches of the government.

In conclusion, we would state that irrespective of all the foregoing, the Subcommittee must recognize that this is a field fraught with danger and this proposed legislation represents an extreme departure from the custom and usage in handling this type of information for the benefit of our country.

Respectfully submitted,

JERRY W. FRIEDHEIM,
*Executive Vice President and General Manager.*

---

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS,
*Washington, D.C., July 24, 1975.*

Hon. FRANCIS X. BELLOTTI,
*Attorney General, Commonwealth of Massachusetts,*
*State House, Boston, Mass.*

DEAR MR. BELLOTTI: I want to thank you again for the testimony on S. 2008 that you gave to my Subcommittee on July 15. As you will recall, we were interrupted for a long period, and I was unable to ask you all the questions that were inspired by your excellent presentation.

For the purpose of completing the record, I hope that you will answer the following questions as soon as possible:

(1) Do you have any reason to believe that the passage of this legislation would hinder law enforcement officials? What has been the effect of the Massachusetts legislation in this regard?

(2) Please describe the powers, activities and findings of the Massachusetts Criminal History System Board. In what ways is it analogous to the Commission created by S. 2008? Do you know of any other States with similar agencies? Based on your experience do you believe that this Commission, as some critics have charged, might become yet another "bureaucratic monster"?

(3) Do you believe that S. 2008 will create undue administrative burdens or prove to be too costly for your state? Will the added costs outweigh the added protections for individual privacy?

(4) Have you had any prosecutions under the Massachusetts statute? Can you provide some examples?

(5) What has been the reaction of the press and the news media in Massachusetts to the limitations imposed by your statute?

(6) From your perspective, do you have any additional comments to make about the message-switching controversy? Would Massachusetts under any circumstances prefer to have the FBI handle this task?

(7) Do you agree with the Justice Department that, in order to protect privacy, it is necessary for State and local governments to dedicate separate computers to the needs of law enforcement agencies?

(8) Can you provide us with a more detailed description of your suit to enjoin the continued operations of NCIC/CCH? What language could we add to S. 2008 that would make your lawsuit unnecessary?

(9) As you know, S. 2008, like most of the privacy legislation that we have been considering at the Federal level, deals almost exclusively with the maintenance and dissemination of information. At some point in the near future, we may have to consider controlling the *collection* of information—an even more difficult problem. Has Massachusetts begun to address this problem, and, if so, can you describe the approach you are taking?

Thank you again for your time and cooperation on this important issue.

Sincerely,

JOHN V. TUNNEY, *Chairman.*

---

THE COMMONWEALTH OF MASSACHUSETTS,
DEPARTMENT OF THE ATTORNEY GENERAL,
STATE HOUSE, BOSTON,
*August 8, 1975.*

Hon. JOHN V. TUNNEY,
*Chairman, Subcommittee on Constitutional Rights,*
*U.S. Senate, Washington, D.C.*

DEAR SENATOR TUNNEY: Thank you for your letter of July 24th. I would be happy to reply to each of the questions you have posed.

1. I do not believe passage of this legislation will impede legitimate law enforcement activities. Law enforcement demands accurate, timely and pertinent data nothing less and nothing more.

Recently, for example, a Federal District Court not only ruled that erroneous FBI NCIC data constituted "a capricious disregard of the rights of the defendant as a citizen," but also ruled that evidence seized as the result of an arrest based on that inaccurate data had to be suppressed. [*U.S.* v. *Mackey*, 43 Law Week 2333 (DC Nev. Jan. 27, 1975)] In short, successful state prosecution was stymied because of the use of inaccurate records maintained by a law enforcement agency, namely the FBI.

I can think of no instances where Massachusetts law enforcement has been impeded because of controls over data imposed by our statute, Chapter 805 of the Acts of 1972. In fact, this law has freed many police departments from the previous practice of acting as credit and character checks for local citizens which was demanded of them by local businesses, licensing boards, officials, and so on.

2. The powers of the Criminal History Systems Board are similar to those of the proposed National Commission. The major exception is that our Board actually administers the Commonwealth's central computerized criminal justice information system.

The Board, in addition, has the authority to regulate all criminal history information systems, automated or manual, throughout the state. The Board certifies all agencies for access rights to criminal history information. Finally, it rules on individual grievances pursuant to Chapter 805.

I do not believe our Board has led to a "bureaucratic monster", and I do not believe the one proposed in S. 2008 will lead to this either. I think the broad-based composition of the Board has guaranteed better regulations, and more effective administration and coordination.

3. I do not believe S. 2008 will constitute an undue expense on the states. The only concern I have in regard to potential costs is the mandatory notification provision to a data subject when his/her data is accessed to an accredited agency.

Such a provision will be costly and cumbersome. I think the individual data subject's right to inspect his/her file any time he/she so desires makes such notification unnecessary.

4. Yes, a state police officer and a private detective were indicted for allegedly disseminating criminal records illegally. The defendants were found not guilty.

In addition, we have had several administrative hearings pertaining to grievances filed pursuant to Chapter 805. For example, recently three teachers contracted to teach at one of our county correctional facilities filed a grievance

alleging that it was illegal for the County Correctional Commissioner to access their files. The Security and Privacy Council heard the case and made a recommendation to the Criminal History Systems Board, which ruled that the Commissioner had legal access to their records. The decision was not appealed to the Superior Court.

5. Generally, the reaction of the media has been very supportive. Individual complaints have been raised from time to time. Recently, reporters complained when the Department of Correction interpreted Chapter 805 to prohibit them from releasing the names of persons on furlough. The Criminal History Systems Board will resolve this issue shortly.

Only the Massachusetts Newspaper Publishers Association has testified against provisions of Chapter 805 before the Legislature.

6. I believe further Federal intrusion into the area of local police telecommunications and message switching to be a violation of the Tenth Amendment to the Constitution. The National Law Enforcement Telecommunications System is entirely capable of handling all present and projected needs of NCIC users.

Any interconnection of local criminal data banks through a Federally controlled telecommunications system will undermine the purpose of S. 2008, namely to guard against the establishment of a Federal criminal data bank.

Finally, as you know, such a Federal role will allow the Federal government to monitor local police communications. Considering that most such communications are not concerning individuals who have violated any laws, such a potential is extremely threatening to personal privacy, as well as local control of local police and criminal justice agencies.

I do not foresee any circumstances which would convince me that the FBI should handle telecommunications.

7. Massachusetts' system is dedicated to law enforcement. I am not expert enough to judge the need for solely dedicated systems to insure system security. I know cost concerns of smaller states over a dedicated system are very real and must be addressed.

8. I believe that when I testified before you I distributed copies of a memorandum prepared by my Office critiquing the legal deficiencies of the current Justice Department regulation of the NCIC/CCH and related manual systems. The points raised in this document would form the basis of any suit in this area.

I think passage of S. 2008 would resolve most of these points, with two possible exceptions. Further Federal intrusion into the area of telecommunications is not prohibited, and unless the National Commission were to act, this would remain a severe legal problem to the states. Second, S. 2008 would permit access to criminal records based on Executive Orders. This could seriously conflict with present Massachusetts law and might present another legal problem for the states.

9. Massachusetts has not addressed this problem specifically either. I agree that it must be addressed in the very near future.

I hope these answers are of help to you and your Committee. If I can provide any more information, please do not hesitate to contact me.

With best wishes,

Sincerely,

FRANCIS X. BELLOTTI.

---

[Additional questions submitted by Chairman Tunney to Harold R. Tyler, with responses.]

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
SUBCOMMITTEE ON CONSTITUTIONAL RIGHTS,
*Washington, D.C., July 18, 1975.*

Mr. HAROLD R. TYLER, Jr.,
*Deputy Attorney General,*
*Department of Justice, Washington, D.C.*

DEAR MR. TYLER: As you will recall, I expressed concern during your July 16 appearance before this Subcommittee that NCIC might be subject to abuse.

I know that you share this concern and will therefore want to investigate thoroughly the circumstances surrounding the attempt to develop a means of using the enormous traffic on the NCIC system for broad intelligence purposes.

The experiment was stopped in early March, 1974 by a combination of concerns stimulated by the Watergate revelations and by Senator Ervin's hearings on criminal justice information systems. I have developed some questions to assist you in investigating this matter.

For background purposes, I refer you to page six of the FBI's message-switching proposal dated April 14, 1975, where mention is made of "flagging" certain records

so a "stop" can be placed against it. Flags would be used, for example, to provide for an indication that a person is wanted for a criminal violation. The proposal notes that the method to be used to place a flag on a file is under active consideration by NCIC.

1. Is the practice of using flags a common practice among criminal justice identification units?
2. Has the FBI used flags in its manual identification operation?
3. If so, what criteria are used to flag an identification card and for whom will the FBI establish a flag in its manual file?
4. Are flags used in the manual system for purposes other than to help locate persons for whom warrants are outstanding? If so, for what purposes?
5. Has the FBI used flags in its NCIC system?
6. What criteria were used to determine which records or individuals were to be flagged in the NCIC system?
7. To what extent could other Federal, State, or local agencies request that flags be placed on the information in the NCIC system?
8. To what extent could divisions within the FBI request that flags be placed?
9. Were flags ever used in the NCIC system for purposes other than to help locate persons with warrants outstanding, such as for allowing the FBI or other criminal justice agencies to know the location of certain persons the agencies had an interest in? If so, please explain what such programs were and their duration.
10. Given the FBI's experience in using flags, what issues are under active consideration by NCIC about their use?
11. Does the NCIC already practice flagging as described in the April 14 plan? If so, then please explain how it works and on which NCIC files such flagging is applicable.
12. Do state and local officials know about such flagging? Do they know when flagging is done?
13. Who contributes to the flag file?
14. What criteria are used to place an individual in your flag file? Are there any members of Congress in your flag file?

I would greatly appreciate answers to these questions as soon as possible, for these answers will greatly assist our mutual efforts to produce effective criminal justice information legislation.

Thank you for your time and consideration, and I look forward to your response.

Sincerely,

JOHN V. TUNNEY, *Chairman.*

---

OFFICE OF THE DEPUTY ATTORNEY GENERAL,
*Washington, D.C., August 29, 1975.*

Hon. JOHN V. TUNNEY,
*Chairman, Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, Washington, D.C.*

DEAR MR. CHAIRMAN: This is in response to your letter of July 18, 1975.

In your letter you expressed concern that there had been an attempt to develop a means of using the message traffic of the National Crime Information Center (NCIC) system for broad intelligence purposes. You requested that I investigate the matter and respond to fourteen specific questions.

I have looked into the matter and the results of my inquiry are reflected in the enclosed answers to the questions you posed. I believe that you will find, as I have, that there has not been any illegal or improper activity in relation to using flagging or other procedures in the NCIC. The specific instance of experimental use of flagging mentioned in your letter is discussed in the answer to question 5.

If you have further questions regarding this matter, please do not hesitate to bring them to my attention.

Your letter of July 25, 1975, has also been received. Answers are being prepared for the forty-three questions posed in that letter and they will be forwarded to you as soon as completed.

Sincerely,

HAROLD R. TYLER, Jr.,
*Deputy Attorney General.*

Enclosure.

ANSWERS TO QUESTIONS POSED IN SENATOR TUNNEY'S LETTER OF JULY 18, 1975

1. Is the practice of using flags a common practice among criminal justice identification units?

Yes. The practice has been engaged in traditionally by law enforcement agencies and has long been recognized as a legitimate law enforcement activity.

A "flag" is no more than a continuing request made by an agency which has authorized access to certain record information. Thus, a police department could properly make an inquiry once each week, day, or hour regarding an individual that agency is attempting to locate for law enforcement purposes. A flag avoids such repetitious inquiries, thereby preventing unnecessary message traffic or correspondence and will result in furnishing no more information than what the agency would be entiled to on an individual inquiry basis.

2. Has the FBI used flags in its manual identification operation?

Yes. The FBI has used flags in its manual identification operation for more than 40 years.

3. If so, what criteria are used to flag an identification card and for whom will the FBI establish a flag in its manual file?

The FBI will establish a flag in its manual identification file for any duly authorized criminal justice agency which requests it for a law enforcement purpose. Typically, flags are established for fugitives, individuals on parole and probation, missing persons, subjects of pretrial diversion, and for investigative purposes.

4. Are flags used in the manual system for purposes other than to help locate persons for whom warrants are outstanding? If so, for what purposes?

Yes. See answer to question 3, above.

5. Has the FBI used flags in its NCIC system?

Yes. However, it is fundamental to an understanding of flags as used in NCIC to recognize that seven of its files (the Vehicle, License Plate, Gun, Article, Securities, Boat, and Wanted Person Files) involve a system of placing flags or continuing notices for agencies which have an investigative interest in stolen property and wanted persons (fugitives). For example, an automobile may be stolen in New Jersey and subsequently recovered in Pennsylvania. Because of the interstate nature of the crime, the FBI and the New Jersey and Pennsylvania police would all have investigative interest in the subject matter. Therefore, an investigative inquiry by the Pennsylvania police to NCIC regarding the vehicle would result in automatic notification to the proper authorities in New Jersey and at the FBI advising that the inquiry was made by Pennsylvania.

As it is not believed that these questions are meant to address the general operations of the NCIC files, as described above, the response to this question, as well as the responses to subsequent questions, will cover only flagging operations that go beyond such general NCIC operations.

In February, 1969, at an NCIC All Participants' Meeting, representatives of the agencies which participate in NCIC requested the FBI to research the feasibility of a program which would allow law enforcement agencies to place flags in NCIC on individuals being sought for law enforcement purposes, but who did not meet the criteria for inclusion in the NCIC Wanted Person File. A warrant must be outstanding for an individual and there must be a willingness to extradite him before his record can be included in the NCIC Wanted Person File. The intent of this request by the NCIC participants was, in effect, to make available in NCIC the flagging services already available in manual identification systems.

Accordingly, during the period April, 1971, to February, 1974, the FBI experimented with the use of flagging procedures on a limited basis in connection with persons and vehicles involved in official FBI investigations. Existence of these procedures was not publicized since they involved a pilot project and because some of the investigations concerned national security matters.

In February, 1974, FBI Director Clarence M. Kelley had the experimental pilot flagging project discontinued. Although recognizing the legitimacy of flags as an investigative tool useful to law enforcement in fulfilling its responsibilities, he

felt that in view of the growing public concern regarding the use of computers, even the legitimate practice of law enforcement in using flags might be misinterpreted and challenged if extended to computer files. He also felt that it would be prudent to first fully examine pending legislation on security and privacy to determine its potential effect. In addition, he instructed that in the future, if any major file or service is added to NCIC, it must be fully disclosed to the public prior to its implementation. Accordingly, notice of the establishment of a Missing Person File in NCIC was published in the Federal Register on May 22, 1975. This File is scheduled to become operational on October 1, 1975.

6. What criteria were used to determine which records or individuals were to be flagged in the NCIC system?

The criteria were: (a) that the subject matter giving rise to the need for the flag must be within the investigative jurisdiction of the FBI, and (b) that it was necessary to determine the whereabouts of the individual involved in order for the FBI to fulfill its investigative responsibilities as prescribed by law.

7. To what extent could other Federal, state, or local agencies request that flags be placed on the information in the NCIC system?

Because this was a pilot program, other Federal, state, or local agencies did not participate in placing flags.

8. To what extent could divisions within the FBI request that flags be placed?

Since this was a pilot program, the placing of flags by FBI Divisions was restricted to a limited number of investigative matters within the Bureau's jurisdiction. The number of active flags never exceeded 4,700.

9. Were flags ever used in the NCIC system for purposes other than to help locate persons with warrants outstanding, such as for allowing the FBI or other criminal justice agencies to know the location of certain persons the agencies had an interest in? If so, please explain what such programs were and their duration.

Yes. Flags were used to help locate individuals in matters wherein the FBI had the obligation to determine their whereabouts in accordance with its investigative responsibilities in both the criminal and national security fields. As indicated in the answer to question 5, such flagging was done on a pilot basis from April, 1971, to February, 1974.

10. Given the FBI's experience in using flags, what issues are under active consideration by NCIC about their use?

Some type of flagging is necessary in NCIC/CCH in order for it to become a complete criminal identification/record system capable of fulfilling all of its responsibilities to law enforcement. For instance, without some form of flagging, there would be no way to notify law enforcement agencies regarding individuals under probation, parole, or pretrial diversion programs who are later arrested. Also, NCIC/CCH would be unable to handle wanted persons who, although the subjects of outstanding warrants, do not fit the criteria for inclusion in the NCIC Wanted Person File.

The subject of flags is discussed on Page 6 of the NCIC Proposed Limited Message Switching Implementation Plan dated April 14, 1975. The issues presently under consideration relative to flagging involve the types of flags to be used, the contents of the flags, the time limit on their validity, and the notification procedure to be used when "hits" are made on the flags.

11. Does the NCIC already practice flagging as described in the April 14 plan? If so, then please explain how it works and on which NCIC files such flagging is applicable.

No, the NCIC does not practice such flagging.

12. Do state and local officials know about such flagging? Do they know when flagging is done?

See answer to question 11.

13. Who contributes to the flag file?

See answer to question 11.

14. What criteria are used to place an individual in your flag file? Are there any members of Congress in your flag file?

No flag file exists in NCIC.

U.S. Senate,
Committee on the Judiciary,
Subcommittee on Constitutional Rights,
*Washington, D.C., July 25, 1975.*

Mr. Harold R. Tyler, Jr.,
*Deputy Attorney General,*
*Department of Justice, Washington, D.C.*

Dear Mr. Tyler: During your July 16 appearance before this Subcommittee, I advised you that I would be sending you questions concerning the FBI's proposal to assume certain message-switching capabilities.

These questions are listed below and, together with your responses, they will be included in the hearing record for S. 2008, my criminal justice information bill.

As you will see, these questions address the merits of the particular configuration for message-switching proposed by the FBI at this particular time. Please remember, however, that Congress should determine policy on issues as significant as message-switching and that, in raising questions about the FBI's specific proposal, I am not precluding other options.

Control over message-switching in a fully matured criminal justice information system conveys such extraordinary power to the controlling agency and carries such serious social implications that decisions about implementation should not be made by executive fiats issued by a single executive agency at the Federal level having a vested interest in the decision.

It is also important that we do not hastily foreclose other options. In this regard, I would point out that studies supported by your Department have examined at least nine different configurations, many of which might be more satisfactory than the one now being promoted so energetically.

I have divided the following questions into six broad categories that are of great interest to the Congress. Each category contains explanatory material along with its specific questions.

DECENTRALIZATION

In line with OMB's recommendation to the Attorney General in 1970, the stated intent of the FBI's latest proposal for handling and storing criminal history information, dated April 14, 1975, is to eventually decentralize the records of most offenders by sending them back to the States. Only for those offenders who committed crimes in more than one state (multi-State offenders) and for Federal offenders would the FBI eventually maintain detailed criminal history records.

However, certain proposals of the FBI bring into question whether, in fact, criminal history records for even single State offenders will initially be more centralized than before.

One issue discussed at the June 11–12, 1975, meeting of the NCIC Advisory Policy Board was that the FBI would convert single-State criminal histories of first offenders for States not yet participating in the CCH system. In view of this proposal, several questions need to be asked.

1. Is the FBI currently converting or planning to convert first time single-State offender criminal history records for States not yet participating in CCH?

2. If so, does the FBI intend to keep the fully converted, computerized single-State records for those States in its own computers until those States are fully able to participate in the CCH system?

3. If yes, doesn't this mean that the FBI will not, in the short run, be decentralizing records, but, in fact, building up a more extensive centralized computerized criminal history file?

The NCIC concept paper, which is included in the FBI's April 1975 message-switching proposal and forms the basis for it, describes a State that is capable of fully participating in the NCIC CCH system as one which:

Maintains a central computerized criminal justice information system interfaced with NCIC.

Has converted an initial load of criminal histories and these records are stored at State and National levels.

Has on-line capability at the State control terminal to enter new records and update computer stored records, and

Allows local agencies to inquire on-line for criminal history at State and National levels.

Five states—California, Florida, Arizona, Illinois and Michigan—are now fully participating in the NCIC CCH system.

4. Are the full records of the single-State offenders from these States being stored as of today in their entirety in the FBI's NCIC CCH file?

5. If the full records are being stored by the FBI, what is the logic of the FBI's stated objective to return such records to the States as soon as they are fully participating?

6. When will the full records be transferred from the FBI to the States and the Single State Offender Record Index be established in the FBI's NCIC CCH file?

7. As new States join the system such as Michigan in May 1975, are their full criminal history records added to the FBI NCIC CCH file? If full records are added to the file, why are they full records instead of index records?

Several additional questions arise as the Subcommittee reviewed the FBI's message-switching proposal which also need clarifying for the Subcommittee to determine whether, in fact, the proposal will, in the near future, result in a decentralization of records.

The plan provides for the establishment of the Single-State Offender Record Index record by a State sending NCIC CCH an empty message containing an identification segment and arrest data on the offender. The plan further provides that the arrest data, except for the State Identification Number, will be stripped off and not entered as part of the Single State Offender Record Index record.

8. Why is the arrest data required to be sent in with the identification segment in establishing the Single State Offender Record Index?

9. Is any use made of the arrest data before it is stripped from the record? If so, what use is made?

The NCIC concept paper which forms the basis for the FBI's message switching proposal states that, in the developed system, the single State records will become abbreviated criminal history records in the National Index and that such records should contain information sufficient to satisfy most inquiry needs such as charges, dates and disposition of each criterion offense, and the offender's current status.

10. How can an abbreviated record containing arrest and disposition data be furnished from NCIC CCH if the arrest data is stripped from the record in creating the Single State Offender Record Index?

11. How will the FBI obtain and keep up to date the current status of the offender.

12. Does this mean that NCIC CCH will be receiving, as a matter of routine, information on each new arrest cycle for an offender thus giving NCIC CCH a full criminal history record. If so, why?

Page 19 of the FBI's April 1975 proposal states that the FBI's Identification Division maintains manual criminal histories which can be converted into computerized records by the States.

13. Are these manual records for single-State offenders going to be given to the States to convert them into computerized full records to be held at State level or will the FBI's Identification Division retain these records?

The FBI's proposal provides for the participation of State Identification Bureaus in establishing and updating CCH records.

14. As part of implementing the CCH system, what consideration has been given to developing the State Identification Bureaus so they will be capable of processing the fingerprint cards?

15. To what extent will Federal funds be used to develop such a State's capability?

16. How does the FBI make the determination that a State Identification Bureau is capable of handling the fingerprint cards? What criteria have been developed to evaluate this capability?

17. When does the FBI anticipate that a majority of States will have this capability?

Page 19 of the FBI's proposal states that the FBI's Identification Division will ultimately become a fingerprint index with its record-keeping function limited to Federal offenders' records.

18. Will the fingerprint cards of single-State offenders presently maintained by FBI's Identification Division be transferred to the States once the State Identification Bureaus are capable of handling them?

19. Have single-State offenders' fingerprint cards been transferred to any State, thus removing them from FBI Identification Division files? If so, which States?

20. Will this transfer be made as each State Identification Bureau acquires the capability or all of the States' Identification Bureaus acquire the capability?

21. Does the FBI's Identification Division presently hold fingerprint cards of multiple-State offenders? If so, will it continue to hold these cards or will they be transferred to the respective States' Identification Bureaus?

22. If the fingerprint cards are transferred, what is the meaning of the statement on page 18 of the FBI proposal that "At least one criminal fingerprint card must be in the files of the FBI Identification Division to support the computerized criminal history record in the index?"

23. Does this mean for multi-State offenders that the FBI's Identification Division will have one fignerprint card to support each arrest recorded in the criminal history?

CCH COSTS

It is recognized by the Bureau, LEAA, and the States, that the successful implementation of a national computerized criminal history system is dependent on the expenditure of significant amounts of funds by the States and the Federal Government. Development at the State level is at various stages. Five States are currently fully-participating in the system. According to FBI estimates, 12 more will become full participants during calendar year 1975. Five have established target dates beyond 1975; twenty-two plan to participate, but have not established target dates; two States do not plan to participate; and the status of five other States is unknown.

According to the FBI proposal, a sophisticated, comprehensive, smoothly running central State identification bureau is imperative to a State's participation in the program. Stages of development range from highly advanced and complex computerized bureaus in Florida and California to a bureau in Vermont operated by one person.

Identification bureau improvement and development of CCH capability at the State level have been supported by two sources of funds—LEAA funding through its Comprehensive Data System (CDS) program (CCH/OBTS is one of five components of the program) and State funds. LEAA fiscal year 1975 funding for CCH/OBTS development through February 19, 1975, was about $6.5 million. The funds were provided to 17 States. However, legislation provides that LEAA funds provided through its CDS program be terminated at some stage in the development of the State programs and the States become self-sufficient in funding the programs.

Under current economic conditions, the lack of general funds within many States limits the amount that can be allotted for CCH development.

24. Since by law LEAA funding of State CCH development is to be terminated after a reasonable time, has the Justice Department determined the point at which developmental funding ceases?

25. Are other sources of Federal funding available to the States for operating their CCH systems once LEAA development funding ceases?

For the 10-year period 1975 to 1984, it seems likely that the survival of the CDS program will require either an increase in Federal funding to more than double the present planned level over the next 10 years, *or* the revision of several high-cost impact CDS policies to reduce the need for Federal funds. During this period, CCH costs will rise to $320 million and the entire CDS to $553 million. One alternative is that the FBI maintain only an index for both single and multi-state offenders, with full records maintained in the State data base. (This is in direct contradiction to the concept embraced in the FBI proposal for a single-State/multi-State configuration of the CCH system.) Has the Justice Department taken this recommendation into account in its consideration of the FBI proposal?

Another less costly alternative would be for the States to automate records for only those subjects whose first arrest occurs after CCH start-up in the State. The current procedure of converting prior manual histories for subjects rearrested after CCH start-up can more than double the number of clerical personnel needed during the first 10 years of CCH operation.

26. Has the Justice Department, in coordination with LEAA and the States, considered this money-saving alternative to the system concept under the FBI proposal?

27. Has the Department of Justice estimated the costs to both the FBI and the States of implementing the FBI proposal?

28. The proposal provides for an FBI audit staff for the CCH system. When will it be established, how large will it be, and how much will its operations cost? If current employees holding other positions are to be used on an as-needed basis, what functions are they currently performing that could be discontinued while they are assigned the audit work?

29. In view of current funding constraints, is it realistic to require the States to use dedicated computers for CCH operations?

30. The FBI proposal as amended at the June 11–12 NCIC Advisory Policy Board meeting contains authority for the FBI to switch administrative messages over NCIC/CCH lines. If NLETS already performs this function, does the FBI need to add this function to its system, with its additional costs?

31. On page 20 of its proposal, the FBI states its costs for implementing and operating message switching. What assumptions were made regarding the determinants of these costs such as the number of States that will be participating and the resulting level of work generated at the main computer at FBI headquarters?

32. Page 3 of the FBI's proposal provides that the details of the single-State/multi-State concept be worked out through meetings of NCIC users. How firm are the FBI's cost estimates for implementing the proposal in view of the fact that the details of implementation will be worked out at these meetings?

TECHNICAL CONSIDERATIONS

At the June 11–12, 1975, NCIC Advisory Policy Board meeting, amendments to message types #3 and #4 were passed to accommodate NLETS representatives present who were concerned that message types #3 and #4 constituted a threat to the existence of NLETS. (See the original types of messages on page 16 of the proposal and the amendment as approved by the Board which is attached.)

33. Explain the differences in the original and the revised message types #3 and #4 and how the revision relieved the NLETS representatives' concerns about the coexistence of their system.

As noted on page 4 of the NCIC concept paper serving as the basis for the FBI proposal, the States would have to enter criminal history data by certain standardized offense classifications.

34. Does the requirement that the State convert its offense classifications to fit into the CCH standardized offense classifications create significant problems for the States?

35. What has the Justice Department done to ensure that the States are converting these offenses to the proper classifications? (If not properly classified, the nature of the offense involved could be misinterpreted by another State which had received the record by message switching over CCH.)

LEGISLATION

Both the FBI proposal and CDS cost study stress the necessity of having 100 percent submission of State and local criminal justice identification, arrest, and disposition data to the State identification bureaus. The FBI proposal requires that the State identification bureau have a fingerprint card on file supporting each data entry into CCH. Many States do not currently have legislation requiring submission of data by local law enforcement agencies. Some States which do have such legislation have experienced problems in enforcement.

36. What is the Justice Department doing to encourage the States to pass such legislation with adequate provisions regarding enforcement?

37. The FBI proposal states that control terminal agencies shall follow the law or practice of their States with respect to purging and expunging CCH data (see page 12 of the concept paper). How many States have laws governing purging/expungment?

38. S. 2008 would create a Commission on Criminal Justice Information with broad powers to issue regulations, interpretations, and procedures relative to CCH operations. In view of the imminent passage of S. 2008, should the Justice Department in the interim give its approval to such a comprehensive policy statement as the FBI proposal?

DEDICATION

The FBI proposal for control of criminal justice systems implies that the hardware, personnel, and management must be dedicated to "service of the criminal justice community." Moreover, the FBI proposal also implies that, in effect, even when a State's criminal justice agencies use equipment and personnel of a noncriminal justice agency for NCIC/CCH purposes, the equipment and personnel should be dedicated to criminal justice purposes.

39. Do you think it is proper for the Federal Government to require the States to adopt management systems, such as dedicated equipment, that may result in an unnecessary expenditure of funds by the States for an effort which is to be of primary benefit to States and which primarily contains State information? Is it technically feasible to design computer programs, even on non-dedicated systems, to assure only proper, authorized access to certain information?

The NCIC concept paper, that forms the basis for the FBI's message switching proposal, notes that even in those States where criminal justice agencies use equipment and personnel of a non-criminal justice agency for NCIC/CCH, the hardware "must be dedicated to the criminal justice function."

40. Doesn't such a requirement, in effect, mean that State criminal justice agencies will not be able to use other State-owned computers unless they are dedicated to law enforcement?

SECURITY AND PRIVACY

The FBI's proposal makes certain provisions for the security of the data and establishes certain conditions required for the switching of CCH records from the record-holding State to the inquiring State. The plan provides that a full record will not be provided in response to a CCH inquiry using other than FBI or State identification numbers (positive identifiers). In this case the FBI forwards from the NCIC/CCH file the identification segment of one or more index records which contain the FBI number on the subjects of the records. According to the plan, the inquiring agency must then compare the pertinent index records with other known data before inquiring for the desired complete CCH record using an FBI or State identification number obtained from the index record of the individual. A summary or full record will be supplied instead of a Single State Offender Record if the FBI or State Identification Number is used in a search.

41. How will the privacy of an individual be protected if the Single-State Offender Record Index record containing the FBI Identification Number is transmitted to the inquiring State based on an initial inquiry?

42. Should several index records be furnished the inquiring State, what will cause the inquiring State to narrow its choices from the Single-State Offender Record Index records furnished? Doesn't this give the inquiring State the opportunity to add to its data base criminal histories for individuals other than the person or persons in custody thus violating the privacy rights of these other individuals?

The FBI's proposal states that the relocation of single-State records to the originating States will further strengthen the control of the States over their criminal history records. However, an inquiry containing the FBI Identification Number will be switched automatically to the record-holding State.

43. How will this control be transferred to the record-holding States if the summary or full record is switched to the inquiring State automatically based on a search with an FBI or State Identification Number?

These questions are designed to give an indication of the problems that have concerned the Congress since the proposal first surfaced last year. Many of us remain concerned about the concentration of too much power in the hands of too few officials and the continuing erosion of State and local autonomy in the criminal justice field.

I look forward to having your responses as soon as possible.

Sincerely,

JOHN V. TUNNEY,
*Chairman.*

OFFICE OF THE DEPUTY ATTORNEY GENERAL,
*Washington, D.C., September 22, 1975.*

Hon. JOHN V. TUNNEY,
*Chairman, Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, Washington, D.C.*

DEAR MR. CHAIRMAN: I am writing in response to your letter of July 25, 1975, in which you raised questions concerning the National Crime Information Center (NCIC) Proposed Limited Message Switching Implementation Plan, dated April 14, 1975.

Our responses to the 44 questions your letter posed are enclosed as separate write-ups. It is noted that, although the letter reflects 43 numbered questions, an unnumbered question appears at the top of page seven.

I have been advised by FBI Director Clarence M. Kelley that on July 30, 1975, you and he, and members of your respective staffs, met to discuss your pending Bill, entitled "Criminal Justice Information Control and Protection of Privacy Act of 1975" (S. 2008). During the discussions, members of your staff expressed interest in learning more about the Department's position regarding the requirement that state and local computer equipment handling criminal history record information be dedicated to criminal justice purposes. Questions 29, 39, and 40 deal with the dedication requirement. We have attempted to provide in our responses to those questions the information that your staff desires.

I greatly appreciate your Subcommittee's interest and concern in this matter. I do hope, however, this communication will provide a better understanding of the rationale behind this Department's position on this very important issue.

If I can be of any further assistance, do not hesitate to contact me.

Sincerely,

HAROLD R. TYLER, JR.,
*Deputy Attorney General.*

Enclosures.

"1. Is the FBI currently converting or planning to convert first time single-State offender criminal history records for States not yet participating in CCH?"

The FBI is not currently converting for entry into the National Crime Information Center (NCIC) first-time, single-state offender criminal history records for states not yet participating in the Computerized Criminal History (CCH) program.

However, the NCIC Advisory Policy Board at a meeting in Kansas City on June 11–12, 1975, approved a plan whereby the FBI would enter into the NCIC CCH File first offender criminal histories encoded by FBI personnel for non-participating states that request it. This procedure would benefit states whose CCH development has been delayed because of budgetary constraints and should help reduce the time it will take for such states to reach full participation by providing cost-free initial files upon which to build their state files. The procedure will also increase the size and geographical coverage of the CCH data base, thereby increasing its utility to all of law enforcement.

This procedure is considered a temporary measure and will continue only until a state becomes a participant. The FBI currently has under consideration a request by Alabama that the Bureau convert and enter Alabama first offender records until such time as that state can assume this responsibility itself. Alabama representatives have advised that they expect their state to become a CCH participant in February, 1976.

"2. If so, does the FBI intend to keep the fully converted, computerized single-State records for those States in its own computers until those States are fully able to participate in the CCH system?"

The FBI intends to keep the full single-state records (containing identification, arrest, and disposition information) it converts for any state in the FBI NCIC computer at Washington, D.C., until (a) the limited message switching capability is operational, and (b) the state has the capability to convert, store, and update its own records. Therefore, the procedure would only be a temporary measure. When the above conditions are satisfied, the FBI NCIC full single-state records will be converted to index records (containing only identification information) and the states will maintain the full records.

"3. If yes, doesn't this mean that the FBI will not, in the short run, be decentralizing records, but, in fact, building up a more extensive centralized computerized criminal history file?"

Yes, it is true that until the NCIC is allowed to acquire a message-switching capability and thereby implement the single-state record storage concept, there will be a continued buildup of full computerized single-state records at the national level. However, if the NCIC Proposed Limited Message Switching Implementation Plan is approved, work can immediately begin on procedures which will eventually result in the decentralization of up to 70% of all CCH records.

"4. Are the full records of the single-State offenders from these States being stored as of today in their entirety in the FBI's NCIC/CH file?"

Yes, the records of single-state offenders entered by all participating states are presently stored in their entirety in the NCIC CCH File, as well as at the state level. As indicated in the response to question 3, the FBI NCIC will have to store full single-state offender records at the national level until such time that it is granted the authority to perform message switching, as that capability is a basic requirement of the single-state record storage concept. Once message switching is implemented, the single-state records at the FBI NCIC will be converted to index records, containing only identification information.

It is noted that in the paragraph just before this question, it was stated that five states, i.e., California, Florida, Arizona, Illinois, and Michigan are participating in the CCH program. As of July 28, 1975, the State of Virginia joined the program, bringing the total to six participating states.

"5. If the full records are being stored by the FBI, why, in light of the FBI's stated objective to return such records to the States as soon as they are fully participating?"

The reason that the FBI NCIC continues to store full single-state records in the national file is that there has been a delay in obtaining authority to implement the message-switching capability required to make the states the source of such records. When such authority is received, it will be possible to begin a program which will eventually result in the "return" of up to 70% of CCH records under the single-state record storage concept.

It should be recognized, however, that actual physical "return" of records will not be required in most instances to implement the single-state record storage concept. This is because the states that participate fully in CCH already maintain computerized counterparts of their records in their own criminal justice information systems. The only exception would be in those few instances where the FBI would, at the request of a nonparticipating state, enter first offender records into the national file until the state becomes capable of CCH participation. At that time, the FBI would send the full single-state records to that state for storage under the single-state storage concept.

Implementation of the single-state storage concept will entail: (1) the conversion of the CCH single-state records at the national file from full records (containing identification, arrest, and disposition information) to index records (containing only identification information); and (2) the implementation of the computer programming capability to switch requests for single-state records from the national level to the state of record and to switch responses from the state of record back through the national index to the requester.

"6. *When* will the full records be transferred from the FBI to the States and the Single State Offender Record Index be established in the FBI's NCIC/CCH file?"

Full single-state records will be transferred by the FBI to the state agencies and the Single-State Offender Record Index established when: (1) authority for NCIC limited message switching is granted; (2) computer programming for limited message switching is implemented at the national level; and (3) the states implement computer programs so they can participate in the single-state record storage concept.

An "Implementation Time Table" is set forth on pages 22–24 of the NCIC Proposed Limited Message Switching Implementation Plan, dated April 14, 1975. That schedule estimated that relocation of single-state records to appropriate states would be accomplished by March 15, 1976. However, in view of the continuing delay in obtaining approval to proceed with the Plan, that date is no

longer valid and no new date can be provided. However, it is estimated that the relocation of the records and establishment of the index would occur approximately eight months after approval was received.

"7. As new States join the system (such as Michigan in May 1973) are their full criminal history records added to the FBI NCIC/CCH file? If full records are added to the file, why are they full records instead of index records?"

As indicated in the answer to question #5, the absence of NCIC limited message switching precludes implementation of the single-state record storage concept. Until NCIC acquires such a capability, it will have to continue maintaining full single-state offender records in the centralized national file. Consequently, as new states, such as Michigan and Virginia, join the CCH program, their full records will be, of necessity, stored in the national FBI NCIC CCH File so that they will be available on-line to all of the NCIC participants. If only index records were stored at the national level and there was no message-switching capability, then only identification information would be available on-line to the NCIC users. Slow and inefficient off-line means would have to be utilized to obtain the arrest and disposition data from the states holding the full records.

"8. Why is the arrest data required to be sent in with the identification segment in establishing the Single-State Offender Record Index?"

The procedure of requiring arrest data with the identification segment was adopted to facilitate state participation in the single-state record storage concept. It was not adopted as a means of collecting detailed arrest data for the national file.

Under the current NCIC CCH record entry procedure, arrest data must accompany each identification segment which is entered. The computers at both the national and state levels are programmed to operate under that procedure. It was decided to retain this procedure in regard to the establishment of index records at the national level.

There were several advantages that prompted the decision. First, the states would not have to deviate from their current operating procedures. Second, they would not have to make costly programming changes to their computers. Third, since arrest data would still be sent to the national level, the State Identification (SID) Number would be made available to the national index. The SID Number is the unique number by which a state identifies a record in its file. The national index would need the SID Number in order to properly address requests it receives for records held at the state level. Since the SID Number is the only part of the arrest data required for the national index, it would be extracted and the remaining data would be discarded.

Since this procedure was adopted as a matter of expediency to facilitate state participation in the single-state storage concept, it is quite likely that a more streamlined procedure will be adopted at a later time as the system evolves.

"9. Is any use made of the arrest data before it is stripped from the record? If so, what use is made?"

As pointed out in the answer to question 8, the State Identification (SID) Number is the only information in the submitted arrest data which is included in the Single-State Offender Record Index (SSORI). The SID Number is the unique number utilized by a state to identify a record stored in its file. Consequently, when the SSORI receives an inquiry on a single-state offender record, it must use the SID Number to request the record from the state holding it, so that the record can be forwarded to the requester via message switching. The other information contained in the arrest data is not used by the SSORI for any purpose and is stripped off and discarded after the index record has been established.

"10. How can an abbreviated record containing arrest and disposition data be furnished from NCIC/CCH if the arrest data is stripped from the record in creating the Single-State Offender Record Index?"

Under the initial concept for record storage adopted by the NCIC Advisory Policy Board, it was envisioned that for each single-state offender record stored at the state level there would be an "abbreviated record" maintained in the national file. This abbreviated record was never definitively described as it was to be adopted only when the single-state/multistate record storage concept was implemented.

The abbreviated record, previously described in general terms in the NCIC CCH Background, Concept and Policy paper, has now been superseded by the Single-State Offender Record Index (SSORI) record as described in the NCIC Proposed Limited Message Switching Implementation Plan of April 14, 1975. As now designed, the SSORI record will contain only identification data.

"11. How will the FBI obtain and keep up to date the current status of the offender?"

NCIC CCH program was designed to decentralize the storage and maintenance of criminal history data. Accordingly, the concept provides for, and requires, the development of strong central state identification bureaus and computerized information systems which have the responsibility for the accuracy, validity, and completeness of the records they enter.

Under the CCH single-state/multistate record storage concept, the maintenance of single-state records of participating states will be the responsibility of the participating states holding the records. Accordingly, reliance is to be placed on those states for on-line entry and updating of the records and for ensuring that the current status of the offender is properly reflected.

In the case of multistate records, the responsibility for maintaining the accuracy, currency, and completeness of such records is to be shared by each participating state which has entered cycles in the records.

All Federal offender records submitted by Federal law enforcement agencies will be maintained and updated by the FBI. These full records will be stored at the national level regardless of whether they are single-state or multistate in nature.

Where arrest data of nonparticipating states has been entered by participating states or by the FBI during initial conversion of a record, the FBI has the responsibility for keeping that data current and accurate until the nonparticipating states become active participants. Similarly, the FBI assists in keeping single-state and multistate records current by updating those records with activity which occurs in nonparticipating states.

"12. Does this mean that NCIC/CCH will be receiving, as a matter of routine, information on each new arrest cycle for an offender thus giving NCIC/CCH a full criminal history record? If so, why?"

The answer is "yes" if NCIC limited message switching is not authorized, and "no" if it is authorized. The single-state record storage concept that would allow for the decentralization of up to 70% of arrest data at the state level can only be implemented if NCIC is authorized to implement a message-switching capability.

Under the single-state record storage concept, after an individual's record is entered as a single-state offender index record at the national level, each subsequent arrest within the entering state will be stored only in that state's file. No subsequent arrest data will be furnished to, or stored in, either the FBI manual Identification Division file or the national NCIC CCH File. Therefore, the national NCIC CCH File will not have the full criminal history records for single-state offenders, or eventually about 70% of all criminal offenders. However, the states will be expected to continue to furnish the national NCIC CCH File for storage of all arrest, court, custody, and supervisory data regarding multistate offenders, who constitute about 30% of all criminal offenders.

"13. Are these manual records for single-State offenders going to be given to the States to convert them into computerized full records to be held at State level or will the FBI's Identification Division retain these records?"

Copies of the FBI Identification Division's manual records (i.e., "rap sheets") are provided to the State Identification Bureaus (SIBs) upon receipt of current arrest fingerprint cards. The originals of these manual records are retained by the FBI Identification Division. The SIBs are free to use the copies of the manual records sent to them for conversion purposes.

"14. As part of implementing the CCH system, what consideration has been given to developing the State Identification Bureaus so they will be capable of processing the fingerprint cards?"

For the CCH concept to operate, each participating State Identification Bureau (SIB) must be able to handle the fingerprint identification function for its state. The FBI assists SIBs to obtain this capability through training and consulting programs.

Upon request, the FBI's Identification Division will provide technical personnel to assist the states in developing their SIBs. Conferences and training sessions are conducted for state personnel during which instruction is furnished concerning the proper processing of fingerprint cards and the recording of arrest disposition data. Similarly, the FBI's Computer Systems Division has, upon request, sent technicians to assist the SIBs in developing the computer aspects of CCH participation.

Recently, in order to give even greater emphasis to assisting the SIBs, the FBI has adopted a "team" approach to providing such assistance. Under the approach, teams of FBI Computer Systems Division and Identification Division technicians, who are knowledgeable in both computer and identification matters, provide on-site instruction to SIBs developing CCH programs. This new program supplements the existing Identification Division's training programs and instructional materials which have been available for many years to state and local law enforcement agencies.

To date, FBI personnel have visited 48 of the 50 states for the purpose of assisting the states to develop their CCH programs.

Under its statutory mandate to fund research and development projects to apply advanced technology to law enforcement operations, the Law Enforcement Assistance Administration (LEAA) has funded several projects with the goal of assisting the SIBs to upgrade their capabilities. Notable among these LEAA projects are: (1) an experiment to determine the feasibility of using holographic (laser) technology for fingerprint identification; (2) an experiment to transmit fingerprint data over a satellite communication system; (3) the funding of private contractors to develop automatic means of recording fingerprints; (4) the development of guidelines for a model state identification bureau; and (5) the recent funding of an operational demonstration of an automatic identification system at the SIB in Arizona.

"15. To what extent will Federal funds be used to develop such a State's capability?"

See answer to question 14 regarding the cost-free FBI assistance provided states, and the research and development projects funded by the Law Enforcement Assistance Administration (LEAA) to assist in upgrading the capabilities of the State Identification Bureaus (SIBs).

"16. How does the FBI make the determination that a State Identification Bureau is capable of handling the fingerprint cards? What criteria have been developed to evaluate this capability?"

The FBI does not make any certification regarding whether a State Identification Bureau (SIB) has the capability of handling fingerprint cards submitted by local contributors. Each state makes its own determination as to whether its SIB is capable of processing the fingerprint cards and accomplishing the identification functions necessary to support CCH participation. However, FBI Identification Division personnel are available upon request to furnish instruction and consultation on such matters, including the establishment of criteria on production and accuracy. This policy has been adopted in order to avoid Federal interference in state administrative matters.

"17. When does the FBI anticipate that a majority of States will have this capability?"

The FBI has not been able to determine when the majority of State Identification Bureaus (SIBs) will have the capability of fully handling fingerprint cards under the CCH concept. However, all states have established SIBs and are working toward full capability.

A fully capable SIB is a prerequisite for state CCH participation. Currently, six states are participating in the CCH program, i.e., Arizona, California, Florida, Illinois, Michigan, and Virginia. Additionally, in a survey conducted by the FBI in March, 1975, another nine states indicated their intention to become CCH participants during 1975.

"18. Will the fingerprint cards of single-State offenders presently maintained by FBI's Identification Division be transferred to the States once the State Identification Bureaus are capable of handling them?"

No, there is no need to transfer such fingerprint cards to the states. Therefore, the FBI Identification Division has no plan to transfer single-state offender fingerprint cards to the State Identification Bureaus (SIBs).

The general practice of law enforcement in fingerprinting an arrestee is to make up two fingerprint cards, one for the SIB and the other for the FBI Identification Division. Therefore, in most states the SIB already holds duplicates of the fingerprint cards presently stored at the FBI.

However, under the CCH concept, fewer fingerprint cards will be forwarded to the FBI by state and local criminal justice agencies in the future. The concept still calls for the preparation of two fingerprint cards on individuals arrested for serious or significant offenses, but both are to be routed to the SIB. The SIB will attempt to identify the individual by comparing the current fingerprint cards with its fingerprint file. If the individual is identified, the SIB will update the CCH File. If, however, no identification can be made at the SIB, the SIB will forward one of the two fingerprint cards to the FBI Identification Division where a search of the national fingerprint file will be made.

It should be noted that where an identification is not made by the SIB, one copy of the fingerprint cards is retained by the SIB for future fingerprint comparisons at the state level, and the other copy is stored at the FBI Identification Division to complete the national fingerprint identification index. Subsequent fingerprint cards received at the SIB regarding that individual can be positively identified through fingerprint comparison without the need to forward them to the FBI. Additionally, the FBI has a set of fingerprints in the national fingerprint index which can be used to identify the individual should he later be arrested in another state.

"19. Have single-State offenders' fingerprint cards been transferred to any State, thus removing them from FBI Identification Division files? If so, which States?"

No. As discussed in the answer to question 18, there is no need and, therefore, no plan to transfer such records.

"20. Will this transfer be made as each State Identification Bureau acquires the capability or all of the States' Identification Bureaus acquire the capability?"

See answers to questions 18 and 19.

"21. Does the FBI's Identification Division presently hold fingerprint cards of multiple-State offenders? If so, will it continue to hold these cards or will they be transferred to the respective States' Identification Bureaus?"

The FBI's Identification Division presently holds fingerprint cards of multiple-state offenders. There is no need and, therefore, no plan to transfer fingerprint cards back to the state level.

At the time of arrest, the usual practice of law enforcement is to make up two fingerprint cards, one for the State Identification Bureau (SIB) and the other for the FBI Identification Division. Therefore, in many states the SIB already holds duplicates of the fingerprint cards stored at the FBI.

Under the single-state/multistate record storage concept, multistate records will be maintained at the national NCIC CCH level. Therefore, it is appropriate that the fingerprint cards which support those records also reside at the national level. However, that is not a requirement, nor will there be any attempt to acquire all such cards for the Identification Division in the future. The CCH concept provides that only the first arrest fingerprint card fom each state is to be sent to the national level (note that the SIB would retain a duplicate copy) and that all cards on subsequent arrests within each state are to be stored at the SIBs. Full CCH records reflect a statement advising that "ARREST DATA BASED ON FINGERPRINT IDENTIFICATION BY SUBMITTING AGENCY OR FBI." This allows for the storage of the fingerprint cards at either the state or national level.

"22. If the fingerprint cards are transferred, what is the meaning of the statement on page 18 of the FBI proposal that 'At least one criminal fingerprint card must be in the files of the FBI Identification Division to support the computerized criminal history record in the index?'"

The FBI will not transfer fingerprint cards now on file at its Identification Division to the State Identification Bureaus (SIBs) for the reason set forth in the responses to questions 18 and 21.

In order to ensure the integrity of its criminal history files, law enforcement long ago adopted the practice of using fingerprint identification procedures to preclude having more than one record in file on the same person or adding arrest information to the wrong record.

Each SIB has the responsibility for performing the fingerprint processing function in regard to its own state file. However, if after a search of its file, the SIB cannot identify an arrestee with a prior record, it will not be able to determine whether the arrestee is a first offender or whether he is the subject of an arrest record in other states without taking additional action.

The SIB could, of course, contact each of the other 49 SIBs to make this determination, but this would be an inefficient procedure. A much more logical and efficient procedure is to establish a central index containing at least one fingerprint card from each state that has an arrest record on the offenders. Then, by making only one inquiry to the central index, the SIB can find out whether a person has ever been arrested elsewhere and, if so, what other SIBs hold records on him.

This is the procedure that has been in existence for over 50 years, wherein the FBI's Identification Division has acted as the national repository for fingerprint records. The advent of computerized records has not changed the need for a national fingerprint index. Accordingly, the FBI Identification Division has been given the responsibility of serving as the national fingerprint index for the CCH program, in addition to its continuing responsibility to perform the same service for the manual records system.

In order for the FBI Identification Division to properly serve as the national fingerprint index, it must receive and retain copies of fingerprint cards representing the first arrest of every offender within each state. If he is a single-state offender, only fingerprint card will be needed at the national index, since he will have a criminal record only in one state. However, if he is a multistate offender, a fingerprint card from each state in which he has a record must be on file at the national index in order to properly link that person to his multistate records.

"23. Does this mean for multi-State offenders that the FBI's Indentification Division will have one fingerprint card to support each arrest recorded in the criminal history?"

No. Under the NCIC CCH fingerprint card concept, the states will submit to the FBI only those fingerprint cards representing the first arrest of each offender within that state. Fingerprint cards for all subsequent arrests of that offender within that state will not be submitted to the FBI but will be retained at the State Identification Bureau.

"24. Since by law LEAA funding of State CCH development is to be terminated after a reasonable time, has the Justice Department determined the point at which development funding will cease?"

No set point for the termination of such funding can presently be established in view of the embryonic state of development of both the national and state CCH programs.

"25. Are other sources of Federal funding available to the States for operating their CCH systems once LEAA development funding ceases?"

There are no known other sources of Federal funding available to the states for operating their CCH systems once LEAA development funding ceases. If a continuing funding requirement arises, it is believed that consideration could be given to either a continuing LEAA-funding program or funding through the FBI's appropriation.

Unnumbered question contained in the first paragraph of Page 7: "Has the Justice Department taken this recommendation ('that the FBI maintain only an index for both single and multi-state offenders, with full records maintained in the State data base') into account in its consideration of the FBI proposal?"

Yes. The single/multistate storage concept embraced in the NCIC Proposed Limited Message Switching Implementation Plan was adopted as a practical matter. The concept will allow for up to 70% of all CCH records (the single-state offender records) to be eventually stored at the state level. The technical problems of automatic storage and retrieval of such records are within the capabilities of the national and state systems. However, the technical problems presented in attempting to store and retrieve records involving offenders with arrest entries in more than one state involve complex techniques which are far beyond the capabilities of the national and state systems. This situation will be under constant assessment and, if and when it becomes practical, the multistate records will also be decentralized to the states.

"26. Has the Justice Department, in coordination with LEAA and the States,

considered this money-saving alternative (automate records for only those subjects whose first arrest occurs after CCH start-up in the State') to the system concept under the FBI proposal?"

Yes. Based upon the results of a cost and benefit study of the Comprehensive Data System, conducted by the Institute of Law and Social Research, LEAA has under consideration the following special condition for possible inclusion in all grant awards relating to Offender-Based Transaction Statistics/Computerized Criminal History (OBTS/CCH) systems:

"No part of project funds, including matching funds, may be used for assembling and converting prior criminal histories—that is, arrests and events prior to OBTS/CCH start up."

The present NCIC CCH conversion policy encourages each state to develop its own criteria for selecting criminal histories for conversion and entry into the CCH File, since the individual states are in the best position to evaluate their own unique needs. However, the states are urged to limit their conversion to active offenders, i.e., those who are the subject of a current arrest or otherwise being processed through the criminal justice system.

"27. Has the Department of Justice estimated the cost to both the FBI and the States of implementing the FBI proposal?"

The current proposal involves the authorization of NCIC limited message-switching capability for the purpose of implementing the single-state/multistate record storage concept, and to allow for on-line "hit" confirmation and NCIC-related management and operational messages. The FBI has estimated its costs in regard to implementing and operating NCIC limited message switching over the first five years to be $1,071,836. Total estimated costs of operating the NCIC, including the CCH program, are submitted annually to Congress as a part of the appropriations process.

The Law Enforcement Assistance Administration recently funded a cost and benefit study of its Comprehensive Data System program. The study, which was conducted by the Institute for Law and Social Research, provided cost estimates on state and Federal participation in the CCH program through 1984.

"28. The proposal provides for an FBI audit staff for the CCH system. When will it be established, how large will it be, and how much will its operations cost? If current employees holding other positions are to be used on an as-needed basis, what functions are they currently performing that could be discontinued while they are assigned the audit work?"

The audit process is already being implemented. Members of the FBI's NCIC staff presently perform the audit function. Their primary duties involve assisting the states to develop their CCH capabilities and auditing is handled as a collateral duty. A total of 48 states have been visited for such purposes to date.

As the state CCH programs mature and shift from a developmental phase to an operational phase, a corresponding shift of effort from development assistance to auditing will occur in the NCIC staff. Therefore, it is anticipated that the growing cost of performing the audit function will be offset by decreases in the cost of assisting the states to initially establish their CCH systems.

It has been estimated that when CCH is fully operational a permanent FBI audit staff of five people could perform the audit function. In addition to the FBI audit staff, special ad hoc audit teams, made up of personnel from the states and the FBI, will investigate alleged security violations discovered by the FBI audit staff. The findings of the ad hoc audit teams will be presented to the NCIC Security and Confidentiality Committee. That Committee will make recommenddations to the NCIC Advisory Policy Board regarding corrective and/or disciplinary action.

The projected annual travel cost of performing the audit function in the fully-developed CCH program has been estimated at $90,000.

"29. In view of current funding constraints, is it realistic to require the States to use dedicated computers for CCH operations?"

Yes. Justification for the requirement of dedication is set forth in the response to question 39. That justification is founded upon a statutory obligation to ensure the security and privacy of criminal history record information. There is, of course, a price that must be paid for security and privacy. However, in the case of dedication, its attainment is a realistic goal and its minimum requirements can be satisfied at a relatively economical cost.

The dedication requirement is set forth in Section 20.21(f)(2) of the Department of Justice Regulations on Criminal Justice Information Systems. That Section requires criminal justice agencies to "Insure confidentiality and security of criminal history record information by providing . . . that where computerized data processing is employed, the *hardware*, including processor, communications control, and storage device, to be utilized for the handling of criminal history record information is *dedicated* to purposes related to the administration of criminal justice." (Emphasis added.)

It is clear from the statements of the critics of dedication that the above wording has been widely misunderstood and, therefore, the requirements for and the cost of implementation of dedication have been exaggerated.

In order to provide clarification to the criminal justice agencies that are affected by the Regulations, the Law Enforcement Assistance Administration (LEAA) on June 30, 1975, issued "Privacy and Security Planning Instructions." These Instructions point out that the Regulations specifically talk in terms of "hardware" rather than "computers" or "computer systems." The reason for this is that the requirement of dedication extends only to those hardware components of a computer (e.g., data storage units, terminals, communications devices, and message processors) which handle and control access to CCH records. This means that the entire computer system need not be dedicated to criminal justice purposes, only those portions dealing with CCH data.

The requirement of dedication can be satisfied by a variety of hardware configurations. An increasingly used approach is to employ a separate small computer engineered to handle the telecommunications function. Such a computer, known as a "front-end," is physically distinct from, but linked to, the main computer system. The front-end is placed under the management control of the criminal justice agency and will handle all requests and responses for CCH records. In view of the low cost of these small computers, dedication is achieved at an economical level.

In order to allow sufficient time for agencies to comply with the dedication requirement, the Justice Department Regulations and the LEAA Instructions provide for an exception to the implementation deadline of December 31, 1977. The Instructions provide that: "State and local agencies may be allowed additional periods of time to implement the dedication requirement upon the submission of a written application to LEAA stating good cause for the extension of the deadline. The fact that the dedication requirement would cause highly excessive increases in present criminal justice systems expenditures constitutes good cause . . . Where it appears that an extension is warranted, States should submit plans, where possible, for reconfiguration of existing hardware in order that dedication can be achieved. Where such reconfiguration is not possible States should submit a brief description of alternative means of compliance in order to provide adequate security protection of criminal history record information."

"30. The FBI proposal as amended at the June 11–12 NCIC Advisory Policy Board meeting contains authority for the FBI to switch administrative messages over NCIC/CCH lines. If NLETS already performs this function, does the FBI need to add this function to its system, with its additional costs?"

In any discussion of NCIC and NLETS, it is important to note that NCIC does not plan to provide general administrative (i.e., free text) message-switching services, such as provided by the NLETS network. NCIC-switched messages will primarily involve formatted messages which relate to CCH and the confirmation of NCIC "hits."

NCIC limited message-switching capability is necessary for CCH to operate under its concept design. The decentralization of records can be effected only if the decentralized records are made easily accessible to authorized agencies through message switching. This accessibility must be tempered by security and privacy considerations and, for this reason, an audit trail is a very necessary system feature. The NCIC message-switching configuration is the only law enforcement telecommunications network which is now capable of maintaining an audit trail on every CCH record dissemination.

Presently, the NCIC system is operated as an inquiry/response criminal justice information system but lacks the means to confirm the validity of NCIC "hits." The "hit" message itself instructs that the recipient of the "hit" should immedi-

ately confirm its status with the agency that entered the record. This must now be performed outside of the NCIC system by telephone, telegram, NLETS message, or other means. The addition of a limited capability will provide the missing link to make the system complete by allowing immediate and efficient confirmation of "hits" on the same system that reported them, i.e., the NCIC.

At a joint meeting of the Board of Directors and Officers of NLETS and the NCIC Advisory Policy Board at Kansas City, Missouri, on June 11–12, 1975, the NCIC Proposed Limited Message Switching Implementation Plan was considered. As a result of these joint deliberations, the Plan was amended to supply specific definitions of the types of messages which NCIC should send over its network. At the conclusion of the meeting, the NLETS and NCIC representatives drafted and executed a joint resolution which expressed support for the amended Plan and recommended its adoption and implementation.

"31. On page 20 of its proposal, the FBI states its costs for implementing and operating message switching. What assumptions were made regarding the determinants of these costs such as the number of States that will be participating and the resulting level of work generated at the main computer at FBI headquarters?"

The cost estimates reflected in the NCIC Proposed Limited Message Switching Implementation Plan are based on the assumption that the participating states will be able to assume the financial responsibility of developing their end of the NCIC system message-switching capability. The Plan was specifically designed to minimize the impact on the states so as to keep state costs to a minimum. See the response to question 8 for an example of how this would be accomplished.

The five-year cost projection figures set forth in the Plan were based on estimates of future message traffic rather than the number of participating states. Traffic was chosen as the parameter for growth projections rather than number of participating states because analysis of Uniform Crime Reporting (UCR) statistics revealed that over 52% of the arrests for 1973 occurred in only eight states. It is believed there is a high degree of correlation between this statistic and projected CCH usage. Accordingly, incremental traffic growth was built into the Plan and estimated traffic at the end of the fifth year was based on CCH being fully operational.

The estimates for the work level at FBI Headquarters were based on the assumption that most of that effort involves implementation of the message-switching capability and that, once implemented, its operation would be handled automatically.

"32. Page 3 of the FBI's proposal provides that the details of the single-State/multi-state concept be worked out through meetings of NCIC users. How firm are the FBI's cost estimates for implementing the proposal in view of the fact that the details of implementation will be worked out at these meetings?"

The estimates are as firm as estimates can be and were arrived at by utilizing the best information available, tempered by the experience gained to date by the FBI's NCIC staff.

As indicated in the answer to question 31, the cost estimates reflected in the NCIC Proposed Limited Message Switching Implementation Plan are based on the assumption that the participating states will be able to assume the cost of developing the NCIC system message-switching capability at their end. The states, however, at future meetings could bring up problems which would require a reassessment of that assumption.

"33. Explain the differences in the original and the revised message types #3 and #4 and how the revision relieved the NLETS representatives' concerns about the coexistence of their system."

The NLETS representatives at the June 11–12, 1975, NCIC Advisory Policy Board meeting were concerned that message types #3 and #4 were unformatted and consequently NCIC users might be tempted to utilize them for non-NCIC-related purposes to the detriment of NLETS.

The revised message definitions, drafted by a conference committee of NCIC and NLETS representatives, describe the exact nature of messages which will be transmitted over the NCIC telecommunications network and, in several cases, specify that they will be formatted rather than free-text messages. For example, before the revisions, the minimum qualification for a type #3 message was that it contain the acronym "NCIC." NLETS was concerned that some NCIC users

would misuse the acronym by sending non-NCIC-related messages over the NCIC network. Consequently, the NCIC agreed to, and did, amend the definition of the type #3 message to eliminate use of the acronym.

The joint NCIC-NLETS resolution was drafted to signify that complete agreement had been reached between the two organizations concerning the NCIC Proposed Limited Message Switching Implementation Plan, as amended.

"34. Does the requirement that the State convert its offense classifications to fit into the CCH standardized offense classifications create significant problems for the States?"

There have been no complaints received that the CCH standardized offense classifications create significant problems for the states. To the contrary, experience has shown that coding personnel have been able to master the uniform codes after a relatively short period of training.

Criminal justice agencies have long recognized the need for the utilization of standardized terminology for interstate understanding and interpretation of offensive charges. To satisfy this need, the NCIC Advisory Policy Board adopted the Uniform Offense Classifications (UOCs) which have been in use since the NCIC CCH File became operational in November, 1971.

Implementation of these uniform codes by the various criminal justice jurisdictions has, of course, required that personnel be trained and indoctrinated in the use and interpretation of the offense codes. The number of UOC codes was limited to a relatively manageable number to cover the large majority of common offenses. Where there is no specific UOC code for a given local offense, the capability of reflecting the literal charge in the record is provided.

"35. What has the Justice Department done to ensure that the States are converting these offenses to the proper classifications? (If not properly classified, the nature of the offense involved could be misinterpreted by another State which had received the record by message switching over CCH.)"

In general, each state is responsible for the the accuracy of its records. However, the FBI assists the states in the following ways:

(a) *Instructional Materials*—State Identification Bureaus (SIBs) and other criminal justice agencies have been furnished complete listings of the Uniform Offense Classifications (UOCs) and written instructions on how to use them.

(b) *Consultation*—The proper use of UOCs is regularly discussed with state representatives during on-site visits by the FBI's NCIC staff. In addition, this matter has received much attention at NCIC conferences and technical meetings, as well as in correspondence with representatives of SIBs and other criminal justice agencies.

(c) *Quality Control Checks*—Both computer and human quality control checks are provided. Whenever a state transmits a record to be included in the national file, the FBI NCIC computer automatically checks each arrest entry to ensure that it includes a valid UOC. The states are encouraged to utilize similar computer checks in their own state systems. In addition, personnel of the FBI's NCIC staff perform selective quality control checks. Whenever a variance is detected between the UOC and local charge of a state record, the responsible state is advised and requested to resolve the difference.

"36. What is the Justice Department doing to encourage the States to pass such legislation ('requiring submission of data by local law enforcement agencies') with adequate provisions regarding enforcement?"

The Justice Department has consistently advocated such legislation and has encouraged its adoption through the following means:

The recently issued Department of Justice Regulations on Criminal Justice Information Systems, Section 20.21(a) (1), state that "Complete records should be maintained at a central State repository . . . and . . . must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred."

The "Privacy and Security Planning Instructions," which were issued by the Law Enforcement Assistance Administration (LEAA) on June 30, 1975, to provide clarification and explanation of the Regulations, suggest that: "States should, therefore, seek legislative authority, where it does not already exist, creating a central repository of criminal history record information. The repository should have the authority by statute to maintain complete criminal history files available to criminal justice agencies throughout the State . . . (E)very

State that does not already have such a law should seek legislation providing for mandatory reporting of dispositions. The legislation should require that dispositions be reported to the central State repository and should be binding on all components of the criminal justice system in the States at whatever level. The legislation should contain sufficient sanctions, including fines, penalties, and audits, to assure that it is enforceable."

In addition to encouraging legislation at the state level, the Department of Justice has also advocated the passage of Federal legislation for the same purposes. Justice Department representatives, including FBI Director Clarence M. Kelley, have in appearances before Congress advocated the passage of Federal legislation for the mandatory reporting of arrest disposition information. The Administration's Bill (S. 1428; H.R. 61) entitled "Crminial Justice Information and Protection Act of 1975," which was drafted by the Justice Department, provides in Section 207(a)(2) for the mandatory reporting of disposition information within 90 days after the disposition has occurred.

"37. The FBI proposal states that control terminal agencies shall follow the law or practice of their States with respect to purging and expunging CCH data (see page 12 of the concept paper.) How many States have laws governing purging/expungement?"

According to the Justice Department's publication entitled "Compendium of State Laws Governing the Privacy and Security of Criminal Justice Information" dated 1975, the following jurisdictions have laws governing purging/expungement:

1. Alaska
2. Arizona
3. Arkansas
4. California
5. Connecticut
6. District of Columbia
7. Florida
8. Hawaii
9. Idaho
10. Illinois
11. Iowa
12. Maine
13. Maryland
14. Massachusetts
15. Michigan
16. Minnesota
17. Missouri
18. New Jersey
19. New York
20. Ohio
21. Oregon
22. Rhode Island
23. South Carolina
24. Tennessee
25. Utah
26. Washington
27. West Virginia
28. Wisconsin

According to the above publication, twenty (20) states have legislation pertaining to the purging of nonconviction records. The purging of nonconviction information means the destruction or return to the individual of criminal justice information where no conviction has resulted from the event which initiated the collection of the information. The process of purging may occur automatically or upon petition of the individual depending upon the statutory provision involved. Expungement has been equated to the purging process, although it could conceivably mean that the records have simply been sealed.

There are seven (7) states which authorize purging of conviction records. The purging of conviction information means the destruction or return to an individual of criminal history information indicating a conviction. Some states purge certain conviction records after a period of time (e.g., 5–10 years) provided the offender has not committed any other crimes following his release.

There are eight (8) states that provide for the sealing of nonconviction information. The sealing of nonconviction information means the removal of criminal history information from active files where no conviction has resulted from the event which caused the information to be collected. Sealing is usually characterized by (a) extraordinary restrictions on dissemination, and (b) physical separation from general files. The process of sealing usually applies to arrest records of individuals whose cases have been terminated by an acquittal or other favorable disposition.

There are seven (7) states that provide for sealing of conviction information. Sealing, like purging may occur either as the result of a petition by the subject or automatically after a specified period of time during which the individual has not engaged in any criminal activity.

The FBI has followed a long-established policy of returning original arrest fingerprint cards to submitting agencies upon notification of sealing action or upon receipt of requests for purging or expungement. This procedure enables the

appropriate sealing action to be taken within the state where the arrest occurred and permits the appropriate agency to effect the purging or expungement action that is required. The return of the fingerprints to the submitting agency results in the complete and automatic expungement of the arrest information from the FBI's files.

"38. S. 2008 would create a Commission on Criminal Justice Information with broad powers to issue regulations, interpretations, and procedures relative to CCH operations. In view of the imminent passage of S. 2008, should the Justice Department in the interim give its approval to such a comprehensive policy statement as the FBI proposal?"

Before answering this question, it should be made clear that the proposal presently under consideration involves only whether NCIC is or is not going to be allowed to perform limited message switching. The FBI was previously authorized by the Attorney General on December 10, 1970, to implement a CCH system. That approval came after the FBI's plans had been reviewed and approved by the affected states, the Law Enforcement Assistance Administration (LEAA), and the Office of Management and Budget. In June, 1971, the Attorney General approved the NCIC CCH Background, Concept and Policy paper which included the single-state/multistate record storage concept. Subsequently, the FBI and the states have worked toward implementing that concept. Message switching is an implicit requirement of the single-state record storage portion of the concept and cannot be implemented without it.

The message-switching proposal has been under consideration for several years now and the lack of a decision has adversely affected the development of the CCH system. The resulting delay and uncertainty have deterred some states from becoming full participants, while those who have proceeded have found it very difficult to formulate plans and budgets for their state CCH systems under such circumstances.

For example, the recently issued Department of Justice Regulations on Criminal Justice Information Systems require the states to submit to LEAA by December 16, 1975, criminal history record information plans. A decision for or against NCIC limited message switching would materially affect how those plans should be drafted. State representatives are becoming increasingly vocal in their demand that the Federal Government make up its mind as it is unfair to the states to ask them to prepare their plans while they remain in the dark as to what course of action the Federal Government will follow.

To postpone the decision regarding message switching until S. 2008 or other Federal legislation is enacted and until the Commission or other type of board is established, would only result in further delay and uncertainty. Further, since there does not appear to be any provision in S. 2008, or the other pending Federal legislation, which would preclude the NCIC from performing limited message switching, there seems to be no need for the Department of Justice to delay its decision until the enactment and implementation of such legislation.

"39. Do you think it is proper for the Federal Government to require the States to adopt management systems, such as dedicated equipment, that may result in an unnecessary expenditure of funds by the States for an effort which is to be of primary benefit to States and which primarily contains State information? Is it technically feasible to design computer programs, even on non-dedicated systems, to assure only proper, authorized access to certain information?"

The Department has a statutory obligation to impose security and privacy requirements on criminal history record information contained in Federally funded state criminal justice information systems. Section 524(b) of the Omnibus Crime Control and Safe Streets Act states that "the Administration shall assure that the security and privacy of all information is adequately provided for and that the information shall only be used for law enforcement and criminal justice and other lawful purposes."

In order to fulfill that statutory requirement, the Department of Justice formulated Regulations on Criminal Justice Information Systems. In drafting the Regulations, the Justice Department was influenced by the following considerations:

It is not technically feasible to design foolproof computer programs to assure only proper, authorized access is gained to a computer system which is accessible through remote terminal devices. However, the problems of preventing unauthor-

ized access are greatly reduced when the equipment providing such access is dedicated to criminal justice purposes and is within the management control of a criminal justice agency.

This fact was recognized in a resolution adopted on May 15, 1967, by the Committee on Uniform Crime Records of the International Association of Chiefs of Police. The resolution stated "that the controls governing access to police information must remain, as they have been historically placed, within law enforcement agencies." Former FBI Director J. Edgar Hoover also took note of this when he stated before the Senate Subcommittee on Constitutional Rights on March 17, 1971, that "If law enforcement or other criminal justice agencies are to be responsible for the confidentiality of information in computerized systems, then they must have complete management control of the hardware and the people who use and operate the system."

Director Hoover's statement and the general concepts of dedication and management control were endorsed by the NCIC Advisory Policy Board and incorporated into the NCIC CCH Background, Concept and Policy paper. Accordingly, the requirements of dedication and management control were adopted in the Department Regulations.

In view of the above, it is believed that the dedication requirement is quite properly a part of the Justice Department's Regulations and that it is necessary to the fulfillment of Congress's directive.

A discussion of the technical requirements and costs of implementing dedication is set forth in the response to question 29.

"40. Doesn't such a requirement, in effect, mean that State crimnal justice agencies will not be able to use other State-owned computers unless they are dedicated to law enforcement?"

No. The technical requirements for achieving dedication are discussed in detail in the response to question 29. Briefly, it should be noted here that there is no requirement that an entire computer system be dedicated to criminal justice purposes. Only those hardware components (e.g., storage devices, terminals, communication devices, and message processors) which handle and control access to CCH data are required to be dedicated. Therefore, state criminal justice agencies will be able to use other state-owned computers and hardware components for operations not related to the CCH function.

"41. How will the privacy of an individual be protected if the Single-State Offender Record Index record containing the FBI Identification Number is transmitted to the inquiring State based on an initial inquiry?"

The privacy of an individual is protected by the fact that arrest information regarding him is not needlessly disseminated to agencies having no interest in him. This is accomplished as follows:

In order for an inquiring agency to get a single-state summary or full record, the agency must request it by using a "positive identifier," such as his FBI Number or his State Identification (SID) Number.

When the inquiring agency knows that an individual has a criminal history record, it can use the individual's FBI or SID Number in its message requesting the record. If the request is for a single-state offender record, the Single-State Offender Record Index (SSORI) will automatically switch the request to the state of record and will switch that state's response (a summary record, a full record, or a "no record") back to the inquiring state.

However, when the inquiring agency does not know whether the individual has a criminal history record, it will not have an FBI or SID Number to use in its request message. Therefore, the agency will have to use "nonpositive identifiers," such as the combination of name, sex, race, and date of birth. Such a request can result in more than one "hit" (response) on records of individuals having similar names and the same sex, race, and date of birth.

Rather than send all of these records (complete with sensitive arrest information) to the inquiring agency, the SSORI wills end the inquiring agency only the index records, which are restricted to descriptive information, such as name, FBI Number, date of birth, place of birth, height, weight, color of eyes and hair, scars and marks, and fingerprint classification. Through a review of the index records that it receives, the inquiring agency can then determine whether any

one of the records contains descriptive information that fits the individual in whom it is interested. If it finds such a record, it can use the FBI Number supplied in the index record (note that the SID Number is not included) to request the summary or full record. Through this procedure those records not fitting the individual's description are not needlessly disseminated, thereby protecting the privacy of the individuals to whom they relate.

"42. Should several index records be furnished the inquiring State, what will cause the inquiring State to narrow its choices from the Single-State Offender Record Index records furnished? Doesn't this give the inquiring State the opportunity to add to its data base criminal histories for individuals other than the person or persons in custody thus violating the privacy rights of these other individuals?"

In regard to the first part of the question, the inquiring agency will find it to its own advantage to follow system procedures. That is, it will find it desirable to narrow its choice by reviewing the several index records furnished and then send a second request to obtain only that record which contains descriptive information fitting the individual in whom it is interested. Otherwise, the agency will find that its computer/terminal equipment and the communications lines linking it to the NCIC national index are burdened down with unnecessary message traffic which degrades service and runs up operating costs. Further, it is quite likely that the ultimate user of the records will not wish to be burdened with large quantities of unwanted and useless information.

Regarding the second part of the question, the procedure which provides that an inquiring agency is to receive only descriptive data in the index records would appear to militate against the agency adding unneeded records to its data base. If the agency desired to obtain more than just the identification portions of the records, it would have to go to the trouble of sending individual message requests for each of the several records. Further, there would be no incentive for an inquiring state to attempt to add out-of-state records to its own data base for the following reasons:

(a) The state computer systems are not programmed to add to their data bases the records they receive from the national level. The states would have to incur the cost and effort of such programming since Federal funding would not be available for this improper purpose.

(b) There would appear to be no advantage to a state to bear the cost of storing records on individuals who have not been arrested in that state. This is especially apparent when one considers the fact that the records are already available to the state through the national CCH system.

(c) If the state did add the records to its data base, it could not be sure that it had the latest arrest and disposition information on the individual since there would be no way that the "bootlegged" copy of the record could be updated with activity which occurred in the state of record. It is noted further that the state storing such records would have to violate the provisions of the Department of Justice Regulations on Criminal Justice Information Systems. The Regulations require agencies to query the central repository prior to disseminating any criminal history record information to assure that the most up-to-date data is being used. However, if the state did comply, there would be no need for it to store the out-of-state data in its own system.

In view of the above considerations, it is believed that there will be no attempts by agencies to acquire records for which they have no use.

"43. How will this control be transferred to the record-holding States if the summary or full record is switched to the inquiring State automatically based on a search with an FBI or State Identification Number?"

Once the single-state records have been returned to the states, the states will have control over their dissemination. Any inquiry containing an FBI Identification Number will be switched automatically to the state holding the record. However, the state has the option whether or not to honor specific record requests since the identity of the requesting agency is a part of the inquiry message. Therefore, a record-holding state will have the ability to control which agencies are to have access to records contained in its system.

○